Information Privacy Bill

As Sent Print

EXPLANATORY MEMORANDUM

General

The Bill establishes a scheme for the regulation of personal information collection and handling in the public sector in Victoria.

Clause Notes

PART 1—PRELIMINARY

Clause 1 sets out the main purposes of the Act.

Clause 2 provides for the Act to come into operation on 1 September 2001 or earlier by proclamation.

It is intended that the Information Privacy Principles and any approved codes of practice will be enforceable following a 12 month transition period (see clause 16). During this time, the Privacy Commissioner will be able to commence programs to raise public awareness about the Act, provide advice to organisations, and register codes. Organisations will be expected to review their systems and procedures to ensure they comply with either all the Information Privacy Principles or an approved code of practice before the end of the transition period.

Sub-clause (2) provides for clause 81 not to come into effect until it is proclaimed. On separate proclamation this amendment will incorporate the Commonwealth's definition of "organisation" so that the operation of this Act and the Commonwealth Act has a defined interface.

Clause 3 defines terms used in the Act.

"Consent" can be express or implied from a particular course of conduct. This may be significant in the context of compliance

with, for example, IPP 2 which allows an organisation to use personal information with the subject's consent.

This would mean, for example, that a person sending a letter to a Minister complaining about a government service in his or her Department would carry an implied consent to use that person's information to investigate the matter.

The definition of "generally available publication" includes information that is generally available to members of the public, whether free of charge or not, and encompasses public registers. While the Act does not apply to generally available publications, it does apply to public registers "so far as is reasonably practicable". The extent to which the administration of, and use of information held on, public registers is governed by the Information Privacy Principles is dealt with specifically in clauses 11, 16 and 18.

The definition of "Information Privacy Principle" (abbreviated in the Explanatory Memorandum and defined in the Act as "IPP") refers to the principles in Schedule 1 of the Act. These principles are adapted from the federal Privacy Commissioner's National Principles for the Fair Handling of Personal Information, on which the Commonwealth Government's private sector privacy legislation is also based. Necessary changes have been made to bring them into a state-based public sector context and to anticipate the introduction of separate legislation for the handling of health information in Victoria.

The definition of "law enforcement agency" includes particular organisations or individuals whose function or functions include law enforcement. The remainder of the definition, paragraphs (f) to (i), is intended to identify organisations by function. It is intended that, where an organisation exercises law enforcement functions, and even where those functions are a small part of the organisation's overall operations, it shall be defined as a law enforcement agency. For example, the Department of Natural Resources and Environment is authorised by its governing legislation to investigate and prosecute specific environmental offences. The Department of Human Services undertakes investigations into notifications of possible child abuse. The definition of law enforcement agency is intended to include such organisations, to the extent of their law enforcement functions.

The exemption available to law enforcement agencies is set out in clause 13. It will only operate in respect of a law enforcement agency's actual law enforcement functions and its community policing functions.

Community policing functions are intended to refer to, for example, investigations about missing persons, lost cattle or, in emergency situations, locating next of kin if required. The term "community policing" is not intended to refer to police work undertaken by members of the community.

The exemption is function-based for two reasons—first, in recognition of the significant number of government agencies which have law enforcement functions and, secondly, to accommodate an increasing diversity of law enforcement functions which extend beyond traditional police powers. In this way, it will have some flexibility to apply to agencies which are given law enforcement responsibilities in the future.

"Organisation" is the term adopted in the Act to identify all entities which are regulated under it. The components of "organisation" are set out in clause 9.

The definition of "personal information" is based on the Privacy Act 1988 (Cth) in the interests of supporting a nationally consistent approach to the protection of information privacy. The definition only applies to information that is recorded in some form. It excludes health information, as defined in Schedule 2 of the Act, in recognition of the tailored treatment being afforded to health records under a separate Victorian Act.

The definition of "public register" includes only those registers the information on which is available to the public, whether free of charge or not. Public register information is recognised in the Act as a generally available publication. However, because of the potential for abuse through, for example, bulk commercial use of information, public registers are not immune from information privacy regulation. Public registers are discussed further under clauses 11, 16 and 18.

The definition of "State contract" refers to a contract under which it is necessary for a contracted service provider to deal with personal information on behalf of an outsourcing organisation. The reference in the definition to "functions" should be construed to refer only to those functions which are

related to the distinctive operations of the outsourcing organisation. It would include the broader role and responsibilities that the organisation has in implementing government policies and delivering government funded services to the community.

Community organisations that are contracted to deliver government funded welfare services, for example, would be required to collect and handle any personal information associated with those services in accordance with the IPP's or an approved code of practice.

Clause 4 guides the interpretation of other terms used in the Act.

Sub-clause (1) provides that the jurisdiction of the Act extends to organisations in Victoria who have possession or control of personal information which may be situated in or outside Victoria.

The definition of "contracted service provider" includes sub-contractors (one or more) who undertake tasks which involve the receipt and handling of personal information.

Clause 5 sets out the objects of the Act. The objects refer a number of times to the handling of personal information. The word "handling" is a general term intended to include all aspects of information management which are regulated by the Act and the IPPs.

Clause 6 describes the relationship of the Act to other Acts.

Sub-clause (1) provides that inconsistent provisions in any other Victorian Act will prevail over any provision of the Act to the extent that they are inconsistent. This will allow relevant aspects of the IPPs to overlay the operation of other Acts where requirements can be observed concurrently.

Sub-clause (2) specifically deals with the operation of the **Freedom of Information Act 1982** (FOI Act). When read with clause 12, it provides that none of the obligations, rights or machinery established under the FOI Act are to be affected by the Act. Any documents which are regulated under the FOI Act will continue to be so regulated and cannot be made subject to additional regulation under the Act.

Clause 7 limits the jurisdiction of the Supreme Court. It states that the Act must be taken not to create any general privacy right or any other rights additional to those which are specifically contained in the Act. Similarly, nothing in the Act is to be construed as giving rise to criminal liability except to the extent specifically described. Clause 72 explicitly states that clause 7 is intended to alter or vary section 85 of the **Constitution Act 1975**.

Clause 8 provides that the Act binds the Crown.

PART 2—APPLICATION OF THIS ACT

Division 1—Public Sector Organisations

Clause 9 lists those entities which are to be taken as falling within the public sector.

Clause 9(1) is drawn so as to ensure that all bodies that should be characterised as "public sector" are included. Moreover, there is flexibility built in to sub-clause (2) to allow, where appropriate, what would otherwise be private sector bodies to be treated as public sector and vice versa.

Personal information collected and handled by members of the Parliament is generally not regulated under the Act as it does not fall within the "public sector". However, Ministers and Parliamentary Secretaries are included in the scheme because of their particular appointment and responsibilities in the Executive. They will be bound by the IPPs to the extent that they collect and handle personal information in this Executive capacity.

Clause 9(2) allows the Governor in Council to include or exclude a particular body from regulation under the Act where required or where the organisation is more appropriately covered under another scheme.

Clause 9(3) only allows the Minister to recommend to the Governor in Council that an Order be made declaring a body to be outside clause 9(1) where the body would be governed by a more appropriate legislatively based scheme. In this way, organisations will not be removed from public sector regulation if the effect would be to exempt them from any data protection or information privacy regulation.

It is envisaged that clause 9 may also be required to manage the interface between the proposed Privacy Amendment (Private Sector) Act 2000 (Cth) and this Act.

Division 2—Exemptions

Clause 10 exempts courts and tribunals from compliance with the Act in respect of the exercise of their judicial or quasi judicial functions. The Act will still apply to personal information collected for other functions, for example, the maintenance of staff records.

Clause 11 grants an exemption in respect of specified types of information that are regarded as publicly available information, including public registers. With limited exceptions, the Act seeks only to regulate personal information that is not publicly available.

Sub-clause (2) refers to the use of information held on a public register. It is intended that the Act will apply so far as is reasonably practicable to personal information held on public registers. Such information stores are collected and held for particular purposes. While public register information should be able to be used for the, or one of the, legitimate purposes for which it was collected, it is intended that the Act will in most cases treat uses outside those purposes as interferences with personal privacy.

For example, it may be an interference with the privacy of an individual for a person to search through the names, addresses and other information held on the Land Register in order to identify and market products or services to a section of the Register that meets a particular socio-economic profile. In these circumstances, the organisation using that information may contravene the Act.

It is envisaged that organisations having responsibility for maintaining public registers will develop codes of practice in conjunction with the Privacy Commissioner to minimise the scope for abuse of public register information.

Clause 12 specifies the relationship between the provisions governing access to information under the FOI Act and the Act. It provides that, for all documents or information that fall within the scope of the FOI Act, IPP 6 or a related applicable code of

practice will not apply. When read with clause 6, there should be no doubt that IPP 6 or a related applicable code of practice will have no effect at all on the scope of the FOI Act.

Clause 13 provides a limited exemption for law enforcement agencies. The exemption does not operate in respect of all IPPs and applies only in relation to the law enforcement and community policing functions of law enforcement agencies. That is, it does not exempt them from complying with all principles in respect of, for example, their own staff records and other administrative matters. Community policing functions, for example, are intended to refer to licensing investigations, location of missing persons, providing necessary responses in public emergency and disaster situations and locating next of kin if required. The term "community policing" is not intended to refer to police work undertaken by members of the community.

PART 3—INFORMATION PRIVACY

Clause 14 states that the IPPs are set out in Schedule 1. The IPPs are adapted from the federal Privacy Commissioner's National Principles for the Fair Handling of Personal Information (the National Principles). The National Principles were developed over a period of about two years in consultation with business and consumer groups. They are widely approved as an acceptable compromise between protection of personal information and use of information for business and other purposes. The proposed Privacy Amendment (Private Sector) Act 2000 (Cth) is also based on the National Principles.

Some modifications to the National Principles have been made to reflect the responsibilities of public sector organisations to promote public interests and be accountable for the expenditure of public funds. Unlike the National Principles, the IPPs do not include provisions specifically for health information. Health information privacy in Victoria is to be regulated by the Health Records Bill, currently under development. In adapting the National Principles under Victorian law it is intended that as much consistency as possible can be maintained with perceptions and practice already operating nationally. Nothing in the IPPs is intended to be taken to override any exemption in Division 2 of Part 2.

Clause 15 deals with the commencement of application of the IPPs. It provides that IPP 1 (the collection principle) and IPP 10 (collection of sensitive information) only apply to information which is collected after the commencement of the Act (1 September 2001). In this way, the Act does not have any retrospective operation. The manner in which information was collected prior to commencement of the Act cannot be made the proper subject of a complaint.

Sub-clause (2) provides that all other IPPs will apply to personal information regardless of when the information was actually collected.

Clause 16 contains the obligation, in sub-clause (1), for organisations to comply with the IPPs in respect of personal information that they handle. Organisations will have to comply from the first anniversary of the commencement of the Act. This phase-in period is intended to allow organisations to assess their data systems, exhaust stationery supplies and put new procedures in place where necessary to comply with the Act. This is the earliest date from which an organisation may be brought to account for contravention of the Act.

There is a qualification to this obligation, described in sub-clause (2). It provides that, where organisations are bound by a contract entered into prior to the date of the second reading speech and the act is done prior to the second anniversary of the commencement of the Act, organisations will not be required to comply with the IPPs to the extent they are inconsistent.

Under sub clause (3) if a contract extends beyond the phase-in period, that period can be extended. To qualify for the extension, an organisation must show that it is doing its best to—

- comply with the IPP's consistent with its obligations under the contract; and
- seek to have the contract re-negotiated to enable the organisation to fully comply with the IPP's.

Sub-clause (4) describes the requirements for administering and using a public register. Although public registers contain information which is available to the public, it is intended that the Act apply to their information "so far as is reasonably

practicable". The rationale behind this policy is explained in relation to clause 11.

Clause 17 deals with the application of the Act to outsourcing arrangements. It is intended that providers of contracted services will be bound under the Act to the same extent as the organisation seeking to outsource one or more functions. The level of obligation will either be according to the default legislative scheme (essentially the IPPs) or an approved code of practice and is linked to acts or practices undertaken for the purposes of the outsourcing contract (the "State contract").

This policy is achieved by allocation of responsibility for any contraventions of the Act which occur in the context of outsourcing. In order to avoid continuing liability for contravention of the IPPs, the outsourcing organisation must ensure two things, set out in sub-clause (4). The first is that a suitable contract is operating to pass that responsibility to the service provider. The contract will specify any particular responsibilities set out in the outsourcing organisation's approved code (if applicable) by which the contracted service provider is to abide. The second requirement is that the IPPs or code must be enforceable against the contracted service provider within the Victorian jurisdiction (see sub-clause (4)(b)). The purpose of this sub-clause is to ensure that individuals whose personal information is misused outside Victoria retain a practical means to address contraventions.

If data handling obligations are not specified in an outsourcing contract the outsourcing organisation will be responsible according to the Act or to the extent specified in an approved code.

Sub-clause (5) excludes the operation of clause 68 to outsourcing arrangements. Clause 68 deals with the liability for contraventions of the Act by employees and agents of an organisation.

PART 4—CODES OF PRACTICE

Clause 18 provides, in sub-clause (1), that an organisation can discharge its duty to comply with an IPP in respect of personal information collected, held, used or disclosed by it through complying with a code of practice approved under this Part.

Organisations which handle personal information are thus given flexibility in the way that they can manage that personal information by developing codes of practice. The scheme allows approved codes of practice to set standards for information handling that differ from the default scheme as long as the standards are at least as stringent as those prescribed by any IPP.

Codes can cover every part of the process of information handling, from collection to complaint handling. Alternatively, they can prescribe procedures in relation to smaller segments of the information handling process and rely on the statutory scheme for the rest. Organisations also have the freedom to adopt a code in respect of a particular type of information they handle. See sub-clause (3).

A code of practice may also—

- address the issue of data matching;
- set guidelines to be followed in determining charges;
- prescribe procedures for dealing with complaints, including the appointment of an independent code administrator;
- prescribe remedies for successful complaints;
- provide for review of the code by the Privacy Commissioner;
- provide for the expiry of the code.

Public sector bodies and councils may use a code of practice, under sub-clause (5), to assist them to discharge their duty to comply with the IPPs "so far as is reasonably practicable" in relation to a public register.

While public register information is publicly available, information privacy issues still arise with respect to public registers because they contain what would otherwise be personal information.

A code of practice would allow agencies and councils to outline how they will manage personal information on a public register responsibly and transparently according to their statutory obligations, and to restrict any potential for abuse. More information about the regulation of public register information is set out in relation to clause 11 and sub-clause 16(4).

Clause 19 sets out the mechanism for gaining approval of a code of practice. This is a formal process reflecting the legal status afforded to codes once they are approved. Sub-clause (1) provides that an organisation may seek approval of a code of practice or of a variation of an approved code of practice by submitting it to the Privacy Commissioner.

If the Privacy Commissioner considers that the code (or variation) is acceptable, he/she will so advise the Minister under sub-clause (3). The Minister may then recommend to the Governor in Council that the code (or variation) be approved, after which the approval would be noted in the Government Gazette.

Sub-clause (3) sets out the main criteria which the Privacy Commissioner must apply when assessing a code or variation. They are that—

- the code or variation is consistent with the objects of this Act;
- the code prescribes standards that are at least as stringent as the standards in the IPPs;
- the code specifies which organisations are to be bound by the code and indicates that the consent of those organisations has been obtained.

Before deciding whether or not to advise approval of a code or variation, the Privacy Commissioner, under sub-clause (4)—

- may consult any other person; and
- must have regard to the extent to which the public has been given an opportunity to comment on the code.

This will not necessarily mean that the Privacy Commissioner or the organisation will need to advertise a code. The circumstances of each application for approval will determine what is adequate.

Under sub-clause (5), a code of practice or variation comes into operation on the day on which notice of approval is published in the Government Gazette or such later day as is expressed in the notice.

Clause 20 describes the procedure for organisations to subscribe to a code of practice that has been approved by the Privacy Commissioner.

Sub-clause (1) provides that an approved code of practice binds any organisation that sought and gained approval of it along with those whose consent was given at the time of approval. Any other organisation may be bound by the code if it states that it intends to be bound by it by notice in writing given to the Privacy Commissioner.

Sub-clause (2) allows organisations to adopt all of an approved code or only certain parts that apply in relation to a specified class of information or activity. A notice given to the Privacy Commissioner under sub-clause (1) may indicate such a qualification. The default scheme (the IPPs) will then supplement obligations in those areas not covered by code provisions.

Clause 21 specifies that an approved code has the same status as the default legislative scheme. That is, any act or practice that is a contravention of a code, even if it does not contravene an IPP, will still contravene the Act.

Clause 22 provides for the Privacy Commissioner to establish a register of all approved codes of practice. Under sub-clause (2), a person may inspect the register and may obtain copies of documents for a fee set down in the regulations.

Clause 23 allows a code of practice to be revoked by the same process as an approval is given in clause 19. That is, the Privacy Commissioner advises the Minister who may recommend to the Governor in Council that a code be revoked.

The Privacy Commissioner may act on his or her own initiative, or on an application for revocation made by an individual or organisation. Before deciding whether or not to advise the Minister to recommend revocation of a code or variation, the Privacy Commissioner, under sub-clause (4)—

- must consult the organisation that sought approval of the code or variation;
- may consult any other person; and

- must have regard to the extent to which the public has been given an opportunity to comment on the code. In relation to this requirement, see also notes for clause 19(4).

Sub-clause (5) provides that a code or variation ceases operation on the day on which a notification is published in the Government Gazette or a later date as is specified in the notice.

Clause 24 preserves the validity of anything done prior to a code being revoked, expiring or ceasing to apply to an organisation. It also allows any proceedings or investigations relating to the period during which the code was operating, which had not been completed (or even commenced), to be completed on the terms of the code as it had operated earlier (sub-clause (1)).

Sub-clause (2) provides that, where there has been revocation of a variation of a code, the code will operate without that variation from the day on which the variation ceases to be in operation. The day a variation ceases, through revocation, is dealt with in clause 23. A variation (or code) may also cease through expiry.

Sub-clause (3) provides that an organisation (or its contracted service provider) will be bound by the original form of an IPP from the time that a code modification to that IPP ceases to operate.

PART 5—COMPLAINTS

Division 1—Making a complaint

Clause 25 prescribes the threshold requirements for making a complaint to the Privacy Commissioner.

Sub-clause (1) allows a complaint to be made in respect of information currently or previously, but no longer, held by an organisation. Sub-clause (2) sets out the circumstances in which a complaint may be made to the Privacy Commissioner, as opposed to a "code administrator".

Paragraph (c) of sub-clause (2) allows a person to make a complaint to the Privacy Commissioner where the person has complained to the relevant code administrator but has not received an adequate response within 45 days. It is not intended that an adequate response would always be resolution of the

complaint. It may be that an adequate response, according to the circumstances, would be a letter explaining, for example, that the complaint had been received but for specified reasons could not be addressed substantively for 60 days. However, it would be expected that some form of contact would be made with the complainant within 45 days.

Under sub-clause (3), it is possible to consolidate complaints so that they may be by one complainant on behalf of others, with their consent. It is envisaged that this would operate in cases where there are substantially the same facts and a common respondent and where resolution of one complaint would be very likely to lead to resolution of all others.

Other sub-clauses deal with formulation of the complaint, including specification of a respondent, assistance to be provided by staff of the Privacy Commissioner, and submission of the complaint to the Privacy Commissioner.

Clause 26 allows the Privacy Commissioner to deal with complaints referred by the Ombudsman.

Clause 27 specifies the manner in which children and people with an impairment may make complaints to the Privacy Commissioner. This clause is based on a similar provision in the **Equal Opportunity Act 1995**.

Division 2—Procedure after a complaint is made

Clause 28 requires the Privacy Commissioner to notify the respondent of a complaint as soon as possible after receiving it.

Clause 29 gives a discretion to the Privacy Commissioner to refuse to deal with a complaint in certain circumstances. Among other things, this clause seeks to ensure that any complaints procedures specified in a code of practice are followed first and that frivolous or vexatious complaints are screened out at the earliest opportunity.

Sub-clause (2) ensures that complainants and respondents are informed of the complainant's right to require the Privacy Commissioner to refer the complaint to the Tribunal for hearing under Division 5.

Sub-clause (3) allows the Privacy Commissioner to refer matters to the Federal Privacy Commissioner or Victorian Ombudsman to ensure that complaints are resolved in the most appropriate forum.

Sub-clause (4) allows the Privacy Commissioner to undertake preliminary investigations to determine whether or not to deal with a complaint, including by inviting any person to attend the office of the Privacy Commissioner or to produce any documents.

Under sub-clause (5) a complainant may, within a specified period, require the Privacy Commissioner to refer a complaint to the Tribunal for hearing. In these circumstances, the Privacy Commissioner must so refer the complaint (sub-clause (6)). The Privacy Commissioner may dismiss complaints which the complainant has not asked to be referred to the Tribunal.

Clause 30 allows the Privacy Commissioner to dismiss a complaint which is subject to a long delay in handling. It is not envisaged that complaints would be dismissed lightly or without attempts by the Privacy Commissioner to locate the complainant or discover the reasons for delay.

Clause 31 allows the Minister to refer a complaint at any stage of its handling to the Tribunal for hearing. It is envisaged that this provision would be used only in cases where the complaint related to an important issue of wider public policy. It is not intended that this clause would give the Minister the power to refer complaints to the Tribunal merely because he or she was actually the complainant or named as the respondent.

Clause 32 gives the Privacy Commissioner the discretion to refuse to hear a complaint on the basis that it is not reasonably possible to conciliate. In such cases, the Privacy Commissioner must notify the parties of this assessment and, if asked in writing to do so, must refer the complaint to the Tribunal for hearing.

Division 3—Conciliation of complaints

Clause 33 requires the Privacy Commissioner to make all reasonable endeavours to conciliate complaints where possible. It is expected that the vast majority of complaints will be resolved by

conciliation. Other provisions in this Division support the requirement set out in this clause.

While it is intended that many complaints will be able to be resolved without the need for the Privacy Commissioner to do so, attendance may be compelled at a conciliation conference, under sub-clause (3).

Clause 34 gives the Privacy Commissioner the power to require any person to provide information or produce documents where the Privacy Commissioner considers that they would be relevant to a conciliation. Clause 34(3) restricts this power in cases where the Secretary to the Department of Premier and Cabinet certifies that the information the subject of a request for production, if included in a document, would be classified as "exempt" under sub-section 28(1) the FOI Act. That sub-section refers to exempt documents which are Cabinet documents.

Clause 34(3) is intended to operate as a supplement to clause 6(2). Clause 6(2) preserves the primacy of FOI procedures over the power of the Privacy Commissioner to compel production of documents (as opposed to information). Where the Privacy Commissioner is seeking to gain access to documents within the purview of the FOI Act, the procedure specified in that Act will continue to be the only enforceable means of access to the documents.

Clause 35 provides a mechanism for enforcement, by registration with the Tribunal, of conciliated agreements. Agreements which are registered are enforceable as orders of the Tribunal. The Tribunal has a discretion to refuse to register agreements in certain circumstances, which does not affect the validity of the agreement but would prevent it from being enforced as an order.

Clause 36 provides that no evidence taken in the course of a conciliation is admissible before the Tribunal unless agreed by all parties. By this clause it is intended to encourage parties to pursue attempts at conciliation fully and frankly.

Clause 37 describes the procedure to be followed in the event that a conciliation fails.

Division 4—Interim Orders

Clause 38 allows a party or the Privacy Commissioner to apply to the Tribunal for an interim order pending further negotiation or conciliation of a complaint. Interim orders may only be made prior to any complaint being referred to the Tribunal.

Sub-clause (3) sets out criteria for the Tribunal to consider in the making of an interim order. In making an interim order, the Tribunal may require an undertaking as to costs and may specify the grounds under which the interim order would be lifted (sub-clause (6)).

Sub-clause (8) provides that this clause is not to have any effect on the Tribunal's jurisdiction to make interim orders under its own Act.

Division 5—Jurisdiction of the Tribunal

Clause 39 sets out the jurisdiction of the Tribunal to hear information privacy complaints.

Clause 40 identifies the proper parties to a complaint before the Tribunal. It is envisaged that the Privacy Commissioner will not generally be a party to complaints before the Tribunal, but may be joined by the Tribunal if required.

Clause 41 puts a limit of 30 days (with possible extension of a further 30 days) for the commencement of the hearing of a complaint referred to it by the Minister under clause 31.

Clause 42 restricts the use of documents produced to the Tribunal which are classified as exempt documents within the meaning of section 28(1) of the FOI Act. Sub-clause (2) allows the Tribunal to make orders about treatment of documents produced. However, in making such an order, the Tribunal must particularly consider sub-clause (4) which highlights the disclosure restrictions which are intended to apply to these documents.

Clause 43 describes what the Tribunal may do after hearing a complaint. In the event that the Tribunal finds a complaint proven, it may make the orders specified under paragraph (a) of sub-clause (1). Under sub-clause (2) these may include orders for correction or

annotation of records of personal information. The Tribunal may also decide, under paragraph (b) of sub-clause (1), to make no order.

If the Tribunal finds the complaint or part of it not proven, it may dismiss it under paragraph (c) of sub-clause (1).

Paragraph (d) of sub-clause (1) gives the Tribunal the power to make an order for reimbursement of the complainant for costs incurred in prosecuting the complaint regardless of the result.

Sub-clause (3) requires the Privacy Commissioner to report any orders relating to public registers to the relevant Minister or council. Under sub-clause (4) the Privacy Commissioner may also make recommendations in the report concerning legislative or administrative action in the interests of personal privacy.

PART 6—ENFORCEMENT OF INFORMATION PRIVACY PRINCIPLES

Clause 44 contains the procedure for the Privacy Commissioner to issue a compliance notice.

The compliance notice is designed to address serious contraventions of the IPPs or a code of practice. Where the Privacy Commissioner is satisfied that an organisation is deliberately disregarding its obligations under the Act or where a breach is particularly serious, he or she is able to direct the organisation to take action within a short period. Failure to comply can incur large penalties.

Sub-clause (1) provides that the Privacy Commissioner may issue a compliance notice where two conditions are satisfied—

- an organisation or contracted service provider has contravened an IPP or an applicable code of practice; and
- the act or practice is a serious or flagrant contravention, or has been repeated on at least five occasions within the previous two years.

A compliance notice requires the organisation to take specified action within a specified period to address the contravention. In circumstances where the specified period is not adequate time to address the contravention fully, an organisation will be required

to give an undertaking to do so within a further specified period (sub-clause (3)).

The Privacy Commissioner may issue a compliance notice on his or her own initiative or through the application of an individual who was a complainant under the Act.

Sub-clause (6) allows the Privacy Commissioner to take into account the extent to which the organisation has complied with a decision of the Tribunal under Division 5 of Part 5 (Tribunal jurisdiction).

Clause 45 gives the Privacy Commissioner the powers to require any person to provide information or produce documents where the Privacy Commissioner considers that they would be relevant to making a decision whether or not to issue a compliance notice. Clause 45(3) restricts this power in cases where the Secretary to the Department of Premier and Cabinet certifies that the information the subject of a request for production, if included in a document, would be classified as an "exempt" Cabinet document under sub-section 28(1) of the FOI Act.

Clause 45(3) is intended to operate as a supplement to clause 6(2). Clause 6(2) preserves the primacy of FOI procedures over the power of the Privacy Commissioner to compel production of documents (as opposed to information). Where the Privacy Commissioner is seeking to gain access to documents within the purview of the FOI Act, the procedure specified in that Act will continue to be the only enforceable means of access to the documents.

Clause 46 gives the Privacy Commissioner the power to examine witnesses through administration of an oath or affirmation where they have been required to attend before the Privacy Commissioner under clause 45.

Clause 47 provides for operation of the privilege against self-incrimination. That privilege allows a person to refuse to answer a question or produce a document where the information given may tend to incriminate the person.

Clause 47 is subject to clause 45, which prevents the Privacy Commissioner from having access to information where the Secretary to the Department of Premier and Cabinet gives a certificate under sub-clause (3) of clause 45.

Clause 48 specifies that it is an offence for an organisation not to comply with a compliance notice. The maximum penalty in the case of a corporation is 3000 penalty units and 600 penalty units in any other case. The **Sentencing Act 1991** (section 110) currently specifies that one penalty unit is $100.

Sub-clause (2) provides that a compliance notice takes effect on the later of—

- the expiry of the period specified in the notice;
- the expiry of any extended period under clause 44(3);
- the expiry of the period within which an application may be made for review of the decision to issue a notice; or
- the determination of a review in favour of the Privacy Commissioner.

Clause 49 provides that an individual or organisation affected by a compliance notice issued by the Privacy Commissioner may apply to the Tribunal for review of the decision to issue the notice. The Privacy Commissioner is a party to a proceeding on a review conducted in relation to this provision (sub-clause (3)).

Sub-clause (2) provides that an application for review must be made within 28 days.

PART 7—PRIVACY COMMISSIONER

Clause 50 provides for the appointment of a Privacy Commissioner.

Clause 51 provides for the Privacy Commissioner to be paid as determined by the Governor in Council.

Clause 52 outlines the terms and conditions of appointment of the Privacy Commissioner, including period of office, terms and conditions, leave of absence and the restriction on engaging in other employment.

Sub-clause (5) provides that, with the exception of section 16(1), the **Public Sector Management and Employment Act 1998** does not apply to the Privacy Commissioner. An amendment to the **Public Sector Management and Employment Act 1998** is made by clause 76 of the Act to give the Privacy Commissioner the function of an "Agency Head" in relation to employees in the office of the Privacy Commissioner.

Clause 53 provides that the Privacy Commissioner ceases to hold office if he or she becomes insolvent, is convicted of an indictable offence or nominates for election for either House of the Parliament of Victoria, the Commonwealth or of any other State or Territory.

Sub-clause (2) specifies that the Privacy Commissioner may resign by notice in writing delivered to the Governor in Council.

Clause 54 contains the procedure for suspension of the Privacy Commissioner from office.

If the Governor in Council uses the power in sub-clause (1) to suspend the Privacy Commissioner, the Minister must provide each House of Parliament with a full statement of the grounds of suspension within 7 sitting days (sub-clause (2)).

Under sub-clause (3), the Privacy Commissioner must be removed from office by the Governor in Council if each House of Parliament within 20 sitting days after the day when the statement was laid before it declares by resolution that the Privacy Commissioner ought to be removed from office.

If the declaration is not made within that time period the Governor in Council must restore the Privacy Commissioner to office (sub-clause (4)).

Clause 55 provides that the Governor in Council may appoint a person to act in the office of Privacy Commissioner during a vacancy in that office; or where the Privacy Commissioner is absent from duty or is unable to perform the duties of office.

Appointment is for a period not exceeding 6 months. The person may not be a member of any Parliament in Australia. The Governor in Council can remove the Acting Privacy Commissioner from office at any time.

A person appointed as Acting Privacy Commissioner has all the powers and must perform all the duties of that office and is entitled to the same remuneration and allowances as the Privacy Commissioner.

Clause 56 provides that an act or decision of a Privacy Commissioner or Acting Privacy Commissioner is not invalid only because of a defect or irregularity relating to his or her appointment.

Clause 57 provides that as many employees as are necessary may be appointed under Part 3 of **the Public Sector Management and Employment Act 1998** for the purposes of the Act.

The Privacy Commissioner may engage as many consultants as are required to perform her/his functions under the Act.

Clause 58 outlines the functions of the Privacy Commissioner, which should not be interpreted prescriptively.

The Privacy Commissioner is given a wide range of functions, including—

- promoting awareness, understanding and acceptance of, the IPPs and their objects;
- undertaking educational programs about information privacy;
- assessing and approving prospective codes of practice;
- providing advice to organisations in relation to development of codes of practice;
- publishing model contractual terms;
- conducting investigations and conciliating complaints;
- advising government on legislation and policies;
- monitoring developments in technology and data processing;
- overseeing/conducting audits;

- examining and assessing the impact of acts of organisations on personal privacy. This function is broad enough to include, for example, the impact of any compliance costs on the manner in which an organisation fulfils privacy obligations under the IPPs or an applicable code.

Clause 59 gives the Privacy Commissioner the general power to perform his or her functions.

Clause 60 provides that the Privacy Commissioner must have regard to the objects of the Act in performing her or his functions.

The objects of the Act are set out in clause 5 and refer, among other things, to the need to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information.

Clause 61 gives the Privacy Commissioner the power to delegate powers under the Act, including, in sub-clause (2), the powers relating to the conciliation of complaints under Division 3 of Part 5.

Clause 62 provides that the Privacy Commissioner must prepare an annual report under Part 7 of the **Financial Management Act 1994** which must include—

- the number of audits conducted in the preceding financial year; and
- the organisations audited.

Clause 63 allows the Privacy Commissioner to provide the Minister with other reports concerning interferences with privacy. The Minister may table a copy of such a report before each House of Parliament.

Sub-clause (3) allows the Privacy Commissioner, in the public interest, to publish reports and recommendations relating generally to the Privacy Commissioner's functions under the Act or to any matter investigated by the Privacy Commissioner whether or not the matters have been included in a report to the Minister.

PART 8—GENERAL

Clause 64 outlines the procedure to be followed in cases where a person is incapable of making a request for access or incapable of accessing his/her personal information or incapable of communicating consent to an act of collection, use, disclosure or transfer of personal information.

This procedure can apply when, as a result of one of the incapacities listed, a person is not capable of understanding the nature of giving consent or making a request for access.

In these cases, an authorised representative can act in the shoes of the individual. Sub-clause (4) ensures that a person can only take action as an authorised representative where the request or consent is not contrary to previously expressed wishes of the individual. The classes of persons who may qualify as authorised representatives are set out in sub-clause (6).

Clause 65 prescribes a penalty for failing to comply with particular requests of the Privacy Commissioner or for obstructing the Privacy Commissioner in the performance of functions.

Clause 66 protects people from liability connected with taking action under the Act.

Sub-clause (1) protects a complainant against actions for loss caused to anyone as a result of the lodging of a complaint.

Sub-clause (2) protects a person against actions for loss caused to anyone as a result of giving any document or information to the Privacy Commissioner.

Sub-clause (3) protects an organisation from liability in any actions for defamation or breach of confidence or criminal offences as a result of the giving of access to information or disclosing information according to the Act (sub-clauses (3) and (4)).

Clause 67 limits the freedom of the Privacy Commissioner (or Acting Commissioner, any delegate, staff member or consultant engaged by the Privacy Commissioner) to deal with information gained while holding that office either during or after the term of the appointment.

Sub-clause (1) prevents the disclosure of information except with the consent of the person to whom it relates, or where the disclosure is for a purpose in the Act.

Sub-clause (2) prevents the Privacy Commissioner from disclosing information gained in the course of a conciliation without first informing the person from whom the information was taken of the intention to do so, and giving that person the opportunity to object to its disclosure. Although the Privacy Commissioner is not obliged to act on any objections, it is expected that these would have a bearing on the decision to disclose or withhold information.

Clause 68 provides that an organisation and not its employee will be responsible for the actions of the employee provided that the employee was operating within the normal scope of his/her employment. An organisation may avoid liability under the Act where it can show that it took reasonable precautions and exercised due diligence to prevent the relevant action from occurring. The equivalent protection applies to agents of a principal organisation acting within their authority. It does not apply to contracted service providers in their capacities as agents of an outsourcing organisation. They are excluded by clause 17(5).

Sub-clause (2) states that where the state of mind is relevant to any inquiry under the Act, the state of mind of an employee or agent can be imputed to the organisation.

Clause 69 allows an organisation to charge a prescribed fee for providing access to personal information.

Clause 70 states that, where an unincorporated organisation is found under the Act to be guilty of an offence, each member of the committee of management of the organisation is to be taken to be guilty of the offence.

Clause 71 deals with the competency of persons to prosecute offences under the Act. This is limited to members of the police force, and the Privacy Commissioner or a person authorised by the Privacy Commissioner.

Clause 72 supports the operation of clause 7 by explicitly noting that, in limiting the jurisdiction of the Supreme Court, it alters or varies the **Constitution Act 1975**.

Clause 73 is the power under which the Governor in Council may make regulations under the Act.

PART 9—AMENDMENT OF CERTAIN ACTS

Clause 74 confers, by amendment to the **Parliamentary Committees Act 1968**, on the Scrutiny of Acts and Regulations Committee, the responsibility to consider future Bills for any adverse effects on personal privacy.

Clause 75 amends the **Magistrates' Court Act 1989**, by including an offence under clause 48(1), namely failure to comply with a compliance notice, as a new offence in Schedule 4 to that Act. Schedule 4 contains a list of offences which are indictable offences triable summarily, with the consent of the accused.

Clause 76 confers, by amendment to the **Subordinate Legislation Act 1994**, on the Scrutiny of Acts and Regulations Committee, the responsibility to consider proposed new statutory rules for any adverse effects on privacy.

Clause 77 amends the **Public Sector Management and Employment Act 1998** by specifying that the Privacy Commissioner has the functions of "Agency Head" under that Act.

Clause 78 inserts a new Part 11A into the **Victorian Civil and Administrative Tribunal Act 1998** to manage actions which are brought in the Tribunal arising under the Act.

Clauses 79 and 80 amend the **Ombudsman Act 1973** to enable the Ombudsman to refer complaints and information to the Privacy Commissioner if appropriate.

Clause 81 contains the mechanism to deal with later commencement of the Privacy Amendment (Private Sector) Act 2000 (Cth). On separate proclamation (see clause 2) this amendment will incorporate the Commonwealth's definition of "organisation" so that the operation of this Act and the Commonwealth Act has a defined interface.

SCHEDULE 1

THE INFORMATION PRIVACY PRINCIPLES

Principle 1 sets out a framework for the collection of personal information, requiring, for example, organisations only to collect personal information which is necessary for their functions. Additional collection requirements specified under IPP 10 apply where sensitive information is being collected.

At the time it is collected or as soon as practicable afterwards, the organisation must take reasonable steps to ensure that individuals know who is collecting their information and why and inform them that they may gain access to it for correction.

Sub-principles 1.4 and 1.5 requires organisations to collect personal information only from the subject of the information where possible or to inform the subject of the collection if information is obtained through a third party.

Principle 2 governs the use and disclosure of information held by organisations. In general, organisations must only use or disclose personal information for the purpose for which it was collected or, otherwise, with the consent of the subject.

However, they are entitled to use or disclose personal information for a secondary purpose where it is related to the primary purpose of collection and the use or disclosure is within the reasonable expectations of the individual. This would be the case, for example, where the information was used to manage, evaluate or improve particular government services in relation to which the information was originally collected.

Secondary uses/disclosures are otherwise permitted in cases where there is a strong public interest in doing so. The remaining paragraphs set out the public interest grounds for secondary use/disclosure. These include, for example, where there is a serious threat to life (d), where disclosure is required by law (f) or for research in the public interest (c).

Paragraphs (g) and (h) of IPP 2.1 give latitude to organisations disclosing personal information to law enforcement agencies. In these circumstances the organisation holding the information would need to be satisfied that the law enforcement agency needed the information for one of the purposes specified.

Minimal information about the purpose of collection by the law enforcement agency would usually be enough to establish that the disclosure was "reasonably necessary". Organisations may, alternatively, seek guidance from the Privacy Commissioner about what assurance they should require before releasing information to such an agency.

IPP 2.1(g) allows an organisation to disclose personal information to law enforcement agencies in these circumstances, however, it is not compelled to do so. In cases where an organisation does exercise this discretion to disclose information, IPP 2.2 requires it to make a note of the disclosure.

Principle 3 is a quality assurance principle seeking to ensure that personal information held by an organisation is accurate, complete and up to date.

Principle 4 requires organisations to protect personal information they hold from misuse, loss, unauthorised access, modification or disclosure. Organisations are also required to take reasonable steps to permanently de-identify personal information or destroy it when it is no longer needed.

Principle 5 encourages transparency by requiring organisations to document clearly their policies on management of personal information and to make those policies available to the public. Organisations must take reasonable steps to let people know, on request, what sort of personal information they hold, for what purpose and how they collect, hold, use and disclose that information.

Principle 6 provides individuals with a right to access their information and make corrections to it, where necessary. In Victoria, the Freedom of Information Act already provides a right of access to documents held by Government. The Bill does not propose to disrupt the established systems of access under this scheme by supplanting them or creating a concurrent system.

Accordingly, in the case of documents held by public sector agencies, the Freedom of Information Act will continue to be the only enforceable method of access. This arrangement is effected by clause 12 of the Bill.

However, Principle 6 applies to organisations which are not included under the Freedom of Information Act. This includes

contracted service providers acting under State contracts. These organisations are required to provide access to personal information unless one of the paragraphs in sub-principle 6.1 applies. In these circumstances, the organisation is still required to consider whether the use of an intermediary would be adequate to satisfy a request for access (sub-principle 6.3).

As an alternative to access in cases where it would reveal evaluative material in connection with a commercially sensitive decision-making process, sub-principle 6.2 allows an organisation to offer an explanation instead of direct access.

Sub-principle 6.4 restricts the scope for organisations to charge for access to the personal information they hold. It is intended that regulations made prescribing fees for access (clause 69) would be consistent with charges under the Freedom of Information Act.

Under sub-principle 6.8, an organisation has 45 days within which to respond to requests for access.

Principle 7 imposes limits on the use of unique identifiers between public sector organisations. It provides that unique identifiers can not be shared by different agencies except with consent of the individual or where it is necessary for their functions. Principle 7 provides a safeguard against the creation of a single identifier which could be used to cross-match data across all Government Departments.

Principle 8 preserves, where lawful and practicable, the right of individuals to remain anonymous in transactions with an organisation.

Principle 9 puts limits on the flow of information outside Victoria. An organisation is only allowed to transfer personal information outside Victoria if it reasonably believes the recipient is subject to a law, or other binding obligation, which imposes restrictions on the use of that information which are substantially similar to the Information Privacy Principles. Personal information may also be transferred with the individual's consent or if the transfer is necessary for the performance of a contract. If consent of the individual cannot practically be obtained, the organisation can only transfer the information if it is for the benefit of the individual and if the individual would be likely to consent.

Principle 10 regulates the collection of sensitive information, providing safeguards which are additional to those set out in IPP 1.

Sensitive information is defined at the beginning of the schedule as information about an individual's racial or ethnic origin, political opinions, membership of a political, professional or trade association, philosophical or religious beliefs or affiliations, membership of a trade union, sexual preferences or practices or criminal record.

In very limited circumstances, under sub-principle 10.2, this information can be collected without consent where necessary for the effective delivery of government welfare programs.