to provide for public access to information held by the public sector, to provide for the correction of personal information held by the public sector, to provide for the responsible collection and handling of personal information by the public sector, to promote appropriate record keeping and record management in the public sector, and for related purposes
# PART 1 – PRELIMINARY

- Purposes and objects
- Freedom of Information
- Information Privacy
- Information Commissioner
- Record keeping and records management
- Definitions
- Other preliminary matters

## PART 2 – GENERAL PRINCIPLES ABOUT DISCLOSURE OF INFORMATION

- Division 1 – General principles
- Division 2 – Accessing government information
  - Subdivision 1 – How is an application made and how is it processed?
  - Subdivision 2 – What decisions may be made in relation to an application?
- Division 3 – Correcting personal information
- Division 4 – Review by public sector organisation
- Division 5 – Miscellaneous

## PART 3 – ACCESS AND CORRECTION RIGHTS

- Division 1 – General principles
- Division 2 – Accessing government information
  - Subdivision 1 – How is an application made and how is it processed?
  - Subdivision 2 – What decisions may be made in relation to an application?
- Division 3 – Correcting personal information
- Division 4 – Review by public sector organisation
- Division 5 – Miscellaneous

## PART 4 – EXEMPTIONS IN THE PUBLIC INTEREST

- Background
- Division 1 – Effect of exemption
- Division 2 – Disclosure generally is not in the public interest
  - Matters Confidential to Government
  - Security and Law Enforcement
  - Secrecy Provisions
  - Preservation of system of justice
- Division 3 – Disclosure in a particular case is not in the public interest
  - Matters affecting relations with other governments
  - Deliberative processes
  - Internal assessment personnel matters and industrial relations
  - Health, safety and the environment
  - Information provided in confidence
  - Privacy and cultural information
  - Trade secrets, scientific research and examination papers
  - Financial and property interests of Territory or public sector organisations
- Division 4 – Exemption certificates

## PART 5 – PROTECTION OF PRIVACY

- Division 1 – Information Privacy Principles
- Division 2 – Exemptions from the IPPs
- Division 3 – Codes of Practice
- Division 4 – Authorisations
- Division 5 – Compliance notices

## PART 6 – INFORMATION COMMISSIONER

- Division 1 – Establishment, functions and powers
- Division 2 – Appointment provisions
PART 7 – COMPLAINTS TO INFORMATION COMMISSIONER .................................................. 20
  Division 1 – Complaints procedure .................................................................................. 20
  Division 2 – Procedure for hearings ................................................................................ 21
PART 8 – APPEALS FROM DECISIONS OF INFORMATION COMMISSIONER ............... 22
PART 9 – RECORD KEEPING AND RECORDS MANAGEMENT ......................................... 23
  Background .................................................................................................................... 23
  Division 1 – Preliminary .................................................................................................. 23
  Division 2 – Obligations of public sector organisations .................................................. 23
  Division 3 – Standards .................................................................................................... 24
  Division 4 – Archiving records ....................................................................................... 24
  Division 5 – Offence ......................................................................................................... 24
PART 10 – GENERAL OFFENCES AND MATTERS RELATING TO LIABILITY ............... 26
  Division 1 – General offences and related procedural matters ....................................... 26
  Division 2 – Legal immunity ........................................................................................... 27
PART 11 – MISCELLANEOUS .............................................................................................. 28
SCHEDULE – INFORMATION PRIVACY PRINCIPLES (IPPs) .......................................... 1
  IPP 1 – Collection .............................................................................................................. 1
  IPP 2 – Use and disclosure ............................................................................................... 1
  IPP 3 – Data quality ........................................................................................................... 1
  IPP 4 – Data security ......................................................................................................... 1
  IPP 5 – Openness .............................................................................................................. II
  IPP 6 – Access and correction ......................................................................................... II
  IPP 7 – Unique identifiers .............................................................................................. II
  IPP 8 – Anonymity .......................................................................................................... II
  IPP 9 – Transborder data flows ...................................................................................... II
  IPP 10 – Sensitive information ....................................................................................... III
INFORMATION BILL: DISCUSSION PAPER

This paper has been prepared for public consultation on the Information Bill. A copy of the Bill is attached to this paper. This paper:

• gives an account of the Northern Territory Government’s information initiatives in relation to FOI, privacy and records management in an Information Bill;
• provides background to the need for an Information Bill;
• raises some key issues regarding the Information Bill; and
• explains the intended operation of the Information Bill.

The paper is not intended to set out the law relating to FOI, privacy and records management. Rather it explains the proposed operation of the Information Bill in plain English, provides a context for the development of an information regime for the Northern Territory and seeks comments on the proposed legislation. All comments received will be taken into account in the finalisation of the Information Bill.

Comments should be directed to:

Director
Policy Unit
Department of the Attorney-General
PO Box 1722
45 Mitchell Street
DARWIN NT 0801

Comments should be provided by 28 February 2001.
INFORMATION BILL

The Information Bill will:

- promote openness and democratic principles in the Northern Territory;
- protect the privacy of personal information held by the public sector;
- ensure that the Northern Territory is well-placed to participate in the Knowledge Economy; and
- promote confidence in the wider community.

The Information Bill has been designed to draw together the related issues of access to government information (“FOI”), privacy and records management legislation in one law in a coherent way. All other jurisdictions in Australia have separate pieces of legislation covering FOI, privacy and records. The result is a less co-ordinated information framework where, for example, FOI legislation may take precedence over privacy legislation. Under the Territory’s proposed information framework, important privacy issues will be taken into account whenever an FOI request involving personal information is made. The appointment of an Information Commissioner to oversee and manage the FOI and privacy components of the Bill will ensure that these issues are dealt with consistently and fairly. No other jurisdiction in Australia has a combined FOI and privacy Information Commissioner. Appointment of an Information Commissioner is a clear indication of the Government’s commitment to a meaningful, low-cost and effective information regime.

Importantly, the Information Bill has been designed to promote the free flow of government information outside of the statutory scheme. This means that, in line with the Government’s pre-election commitments, the information regime will indeed be a “force for disclosure”.

The Information Bill will provide the Northern Territory public sector with a framework within which it can maximise its use of information and communications technologies. As such, it will facilitate consumer and business confidence and trust in the Government’s ability to participate in the Knowledge Economy as well as giving legislative backing to the responsible and effective management of government information. This new legislative framework will ensure that the Northern Territory public sector can perform effectively in a networked, global economy while delivering improved protection for, and access to, government information in the Territory. In essence, the Information Bill is concerned with the good management and responsible custodianship of government information.
PART 1 – PRELIMINARY

The Information Bill will come into operation on a date fixed by the Administrator by notice in the Gazette (clause 2). It is intended that, following completion of this consultation process, the Bill will be finalised and then, subject to Cabinet approval, introduced at the next sittings of the Legislative Assembly.

Purposes and objects

Clause 3 outlines the purposes and objects of the Information Bill. The purposes set out what the Bill does (clause 3(1)) while the objects set out what is intended to be achieved in carrying out those purposes (clause 3(2)). The purposes of the Information Bill are to:

- provide the public with a right of access to government information (FOI) except where certain limited exceptions to that right of access exist. Individuals will also have a statutory right to seek access to, and correction of, personal information where it is inaccurate;

- ensure that the privacy of personal information in the public sector is protected subject to balancing the public interest in the free flow of information against the public interest in the protection of personal information. This will be achieved by applying Information Privacy Principles to the collection and handling of personal information unless specifically exempted;

- provide for the appointment of an independent statutory officer, the Information Commissioner, to oversee the freedom of information and privacy regime. The Information Commissioner may receive, investigate and mediate complaints and is able to make final, binding determinations if mediation fails; and

- set out the record keeping and records management responsibilities of the public sector.

The objects of the Bill are to:

- encourage the widespread publication of government information;

- encourage accountability in government by providing the public with a right of access to government information;

- balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information; and

- promote efficient and accountable government through improved record keeping and records management.
Clause 3(3) provides that the Bill will not replace other existing or future procedures for accessing government information and will not limit in any way access to government information (other than personal information) that is publicly available. This will ensure that the FOI provisions of the Bill do not become a default access regime, preventing people from gaining access to government information unless they work their way through the formal access procedures outlined in this Bill.

**Freedom of Information**

Freedom of information is about providing citizens with a right of access to government information in order to enhance the openness and accountability of government and to promote public participation in policy and decision-making. It also encourages an environment of transparency and openness that is conducive to the establishment and maintenance of business and consumer confidence by demonstrating that government processes and procedures are open to scrutiny. It is widely recognised that a transparent and certain legal environment plays an important role in attracting and retaining both national and international investment.

Many FOI models are overly complex and adversarial in nature, encouraging confrontation and litigation. The Information Bill has been developed against a background of the growth of the Knowledge Economy, the experience of other jurisdictions and the Territory’s own unique needs. Importantly, it has been designed *not* to encourage confrontation and litigation.

**Information Privacy**

Privacy is a broad concept that deals with freedom from intrusive behaviour. A specific subset of privacy is data protection or information privacy, which deals with the control, collection, use and disclosure of personal information. Privacy legislation in Australia is primarily concerned with the protection of personal information. Lack of protection for personal information has consistently been identified as one of the most significant impediments to the growth of electronic commerce and the electronic delivery of government services. Currently, there is no comprehensive privacy scheme in place in Australia.

The Northern Territory’s proposed public sector privacy framework will support the federal government’s legislative initiative to extend privacy protection to the private sector, thereby ensuring a seamless framework of information privacy protection in the Territory. This will ensure equivalent protection of personal information regardless of whether a public or private sector organisation is involved.
Information Commissioner

The Information Commissioner will play a crucial role in upholding the objects of the Information Bill. The Information Commissioner will oversee the FOI and privacy components of the Bill and his or her responsibilities will include education, development of guidelines, investigation and mediation of complaints and making final determinations where mediation is unsuccessful.

International experience shows that a focus on education and mediation coupled with meaningful enforcement powers produces effective and practical information outcomes. The Information Commissioner will be an independent arbiter, capable of resolving any disputes that arise under the Bill.

Record keeping and records management

Information legislation must be underpinned by an effective records management strategy to keep costs down, to ensure the better management of records and to drive effective implementation. The Information Bill’s FOI regime, for example, requires records to be accessible. While the majority of the functions of the records management strategy do not require legislation, laws that set out the record keeping and records management responsibilities of government agencies are necessary. These will cover issues such as protecting records, making and keeping accurate records of activities, establishing and maintaining a records management system, monitoring and reporting on the system and keeping technology-dependent records accessible. There will be considerable efficiencies and cost savings to Government in using the scheme that has already been developed by the Northern Territory Archives Service to support the Information Bill’s records management provisions.

Definitions

There are a number of key definitions in the Bill (clause 4). These include the following.

- **Personal information** is information contained in a record that is held by or on behalf of a public sector organisation and from which a person’s identity is apparent or reasonably able to be ascertained. This definition is central to the Bill’s regime for the protection of the privacy of personal information.

- **Code of practice** forms the basis for permitting the development of privacy rules that are tailored to meet the specific requirements of particular agencies or activities. These codes must be consistent with the objects of the Bill.

- **Consent** means consent whether express or implied. This may be significant in the context of compliance with, for example, Information Privacy Principle 2,
which allows a public sector organisation to use personal information with the person’s consent.

- **Contract service provider** means the person or body who is collecting or handling personal information under a service contract. This is a key definition in relation to the Bill’s proposed coverage of outsourcing arrangements and should be read in conjunction with clause 145 and the definitions of “outsourcing organisation” and “service contract”.

- **Outsourcing organisation** means the public sector organisation for whom, or on whose behalf, personal information is collected and handled under a service contract.

- **Service contract** means a contract or other arrangement entered into after the commencement of the regime under which a person or body handles personal information for or on behalf of a public sector organisation.

- **Public register** is a register that satisfies a two-part test, being a register that contains personal information that a person or body was required or permitted to give to a public sector organisation and which is made available for inspection by members of the public. Under clause 66 a public register is to be kept in compliance with the Information Privacy Principles to the extent that it is practicable to do so given the requirements imposed for the keeping of the register.

- **Law enforcement agency** is defined broadly to include the Northern Territory Police Force and the police force of the Commonwealth, a State or another Territory as well as the National Crime Authority. It also covers any body established by a law in force in the Territory that performs functions such as preventing, detecting, investigating, prosecuting or punishing the commission of offences; managing property seized or restrained under a law relating to the confiscation of the proceeds of crime; protecting the public revenue; and executing or implementing a decision, direction or order of a court or tribunal, including executing warrants.

- **Health information** is an expansive definition that is designed to cover all types of personal information relating to a person’s health, including personal information relating to a person’s physical, mental or psychological health, a person’s impairment, personal information connected with the delivery of a health service and genetic information. By virtue of IPP 10, health information is a category of sensitive information and is given a higher level of privacy protection under the Bill. It should, however, be noted that the Government is concerned to ensure that health information should be subject to the same privacy protection irrespective of whether it is collected and handled by a public or private sector organisation. The Bill only applies to the public sector. The government will closely consider the need for specific, stand-alone health privacy and records
legislation that ensures that the health information of Territorians is given the same privacy protection across the whole of the private and public sectors.

- Unique identifier is a code (other than a person’s name) assigned by a public sector organisation to identify a person. This definition is important in terms of Information Privacy Principle 7 – Identifiers.

“Public sector organisation” is defined by clause 5. Public sector organisation is defined broadly so as to encompass the full range of government organisations. It includes an Agency, a local authority, a statutory corporation, the Police Force of the Northern Territory and a court or tribunal of the Territory. Government Business Divisions (GBDs) will be covered in relation to privacy and records management but not in relation to FOI. GBDs are intended to operate in a commercial context in competition with the private sector. As the private sector is not currently subject to FOI legislation it was considered inappropriate to apply the Bill’s FOI provisions to GBDs. However, under the Bill’s privacy provisions, individuals will be able to seek access to, and correction of, personal information held by GBDs.

A public sector organisation also includes Ministers and Parliamentary Secretaries. Ministers and Parliamentary Secretaries will be covered by the FOI and privacy components of the Bill, but only to the extent that they hold government information in connection with their responsibilities as the holders of that office.

Other preliminary matters

Clause 6 guides the interpretation of other terms used in the Bill. It provides that a public sector organisation “holds” personal information if it has possession or control of the information. The jurisdiction of the Bill will extend to public sector organisations in the Northern Territory who have possession or control of personal information that may be situated in or outside the Northern Territory.

The nature of the rights created by the Bill will be restricted to those outlined in the Bill (clause 7). That is, the Bill must not be taken to create any general privacy right, for example, or any other rights additional to those that are specifically contained in the Bill. Similarly, nothing in the Bill is to be construed as giving rise to a criminal liability except to the extent specifically described.

The Bill will bind the Crown (clause 8) and if there is an inconsistency between the Bill and another Act, the other Act will prevail to the extent of the inconsistency (clause 9).
PART 2 – GENERAL PRINCIPLES ABOUT DISCLOSURE OF INFORMATION

Pro-disclosure

The statutory access regime provided by the Bill will not displace existing means of gaining access to information. In fact, the regime is based on a policy of pro-disclosure (clause 10). The public sector will encouraged, wherever possible, to publish a wide range of government information as a matter of course (clause 10 (1) and (2)). Access to information may only be denied when there is an exemption or a countervailing public interest. Despite the existence of exemption categories, the Information Bill states that nothing in it is intended to prevent or discourage public sector organisations from disclosing records (including exempt records) where they can properly do so (clause 10(2)).

Publication

The Bill provides that each year public sector organisations must publish information about their structure, functions and the kinds of government information they hold (clause 11). Organisations must also provide information about a contact officer to whom an initial inquiry about seeking access to government information may be made and how to lodge a request under the Bill (clause 11 (1)(c) and (d)).

Application

Clause 13 provides that government information (other than personal information) is subject to FOI if it was created up to five years before the regime commences. However, government information may also be subject to FOI if it is reasonably necessary to enable a person to properly understand information to which the person has been provided with access under the Bill (clause 13).

Clause 14 provides that personal information is subject to the access and correction provisions and the privacy provisions of the Bill regardless of when it was created or received by the public sector organisation. However, the collection provisions only apply to personal information collected after the regime commences.
PART 3 – ACCESS AND CORRECTION RIGHTS

Division 1 – General principles

This Part of the Bill outlines how the rights of access to, and correction of, government information will work. A person will be entitled to access government (other than personal information) if the person is an Australian citizen or a permanent resident (clause 15). Any person will be entitled to access, or to correct, his or her personal information (clause 16). If there is a disagreement about the correction of personal information, the person may request the public sector organisation to take reasonable steps to append a statement prepared by the person outlining why he or she considers that the information is inaccurate, incomplete or out of date, to the information (clause 16).

Clause 17(1) requires public sector organisations to deal with applications promptly, efficiently, fairly and openly. In dealing with applications public sector organisations are not to be concerned about, or to take into consideration, the reason access is sought (clause 17(2)). It is a fundamental principle of FOI that the applicant does not have to establish standing or an interest in order to exercise his or her statutory rights.

Division 2 – Accessing government information

Subdivision 1 – How is an application made and how is it processed?

This part of the Bill covers procedural matters in relation to applications for access to government information, including the need for applications to be in writing (clause 18). Responses to applications must be made within 30 days (clause 19) and must provide applicants with a formal notice of decision in relation to access applications (clause 20).

Subdivision 2 – What decisions may be made in relation to an application?

This part of the Bill covers what decisions may be made in relation to access applications. Access may be provided in whole or in part (clause 21) or in edited form (clause 22). Access may also be deferred for a period not exceeding 60 days for a range of reasons including if the information is to be published but is not yet published (clause 23). Access may also be refused if the information is subject to an exemption under Part 4 of the Bill (clause 24).

Where a public sector organisation needs more than 30 days in order to make a decision about an access request, it must notify the applicant (clause 25(1)). Additional time may be necessary for a range of reasons, including that a large amount of information is required, an extensive search is required or compliance within 30 days would unreasonably interfere with the operations of the organisation (clause 25(2)). Where information cannot be identified or found or it does not exist, the organisation
must inform the applicant (clause 26(1)). If this occurs, the public sector organisation is to be taken to have refused access to the information for the purposes of the Bill (clause 26(2)).

In cases where a public sector organisation decides that it does not hold information because it knows or believes on reasonable grounds that another public sector organisation holds it, the application must be transferred (clause 27). The transfer must occur within 15 days of receiving the application (clause 28).

The statutory access regime will include provisions to protect the rights of third parties (clause 29). This is sometimes called “reverse FOI”. Reverse FOI means that individuals or organisations are given an opportunity to say whether or not information relating to them should be disclosed under the access regime. If access is to be granted, third parties are given an opportunity to complain to the Information Commissioner about decisions that affect them and to seek to ensure that the information is not released. Reverse FOI will apply to the following categories of third party information: personal information, Aboriginal sacred sites or tradition, trade secrets and business, commercial or financial information (clause 29).

Division 3 – Correcting personal information

The procedural provisions in relation to correcting personal information are designed to mirror, so far as is appropriate, the Bill’s provisions in relation to access to government information. This includes making an application (clause 30), responding to applications (clause 31), correcting information (clause 33), refusing to correct information (clause 34), taking extra time (clause 35) and transferring applications (clause 36).

Division 4 – Review by public sector organisation

This part of the Bill sets out the regime for internal reviews of access and correction decisions. In essence, applications for internal review must be made within 30 days after being notified of the decision (clause 37) and the internal review must take place within 30 days of receiving an internal review request (clause 38). Internal reviews may confirm or vary the initial decision in whole or in part, revoke it in whole or in part, or substitute another decision that could have been made under the Bill (clause 39). The outcome of an internal review must be notified to the applicant and must contain the reasons for decision (clause 40). The notice must also inform the applicant that he or she has a right of complaint to the Information Commissioner under Part 7 of the Bill (clause 40).

Division 5 – Miscellaneous

This part of the Bill deals with vexatious applicants. It enables public sector organisations to seek a declaration from the Information Commissioner that a person is a vexatious applicant (clause 41). The Commissioner may only make such a
declaration under certain conditions, including where repeated applications are made for the purpose of harassing, obstructing or otherwise interfering with the operations of the organisation (clause 41). A declaration has effect subject to the terms and conditions specified by the Commissioner. This may include a condition that a vexatious applicant is restrained from making access applications to public sector organisations without the written permission of the Commissioner.
PART 4 – EXEMPTIONS IN THE PUBLIC INTEREST

Background

The principles that underpin FOI have been recognised as essential to the effective operation of democracy, and FOI legislation has been widely accepted as an integral part of open and accountable government. The policy that underpins FOI legislation is that it is in the public interest for government information to be made available to the public.

Whilst FOI laws worldwide recognise the public interest in freedom of information, the right is not an unfettered one. Sometimes the public interest can only be served by keeping information secret. All FOI laws seek to balance conflicting notions of the public interest by permitting the disclosure of information but exempting certain categories of information from disclosure. Determining where the balance lies is always a matter of vigorous public debate.

On the whole, it is assumed that it is in the public interest for an individual to have a right to access government information and it is the responsibility of government to claim that a particular exemption applies in a specific case. Public interest tests are also built into many exemption provisions. Exemptions may be divided into three broad categories:

• Protection of government interests (eg. law enforcement, public safety, financial)
• Protection of third parties (eg. business affairs, personal affairs, adoption)
• Functions of other bodies (eg. legal professional privilege, contempt of court)

However, there are some categories of information that are considered so sensitive that they attract unqualified protection. Two examples are (1) national security and defence, and (2) Cabinet documents. In Australia these categories are not usually subject to a public interest test, and an exemption certificate attesting to a document’s protected status is usually available. An exemption certificate is effectively a ‘Ministerial veto’ and cannot be revoked or reviewed by an appeal body (eg. the AAT at Commonwealth level).

The way in which exemptions are expressed differs from jurisdiction to jurisdiction. However, there is a significant degree of uniformity in the substance of the matters covered by exemptions. An account of the exemption categories contained in the Information Bill is provided below.

Division 1 – Effect of exemption

Clause 42 of the Bill provides that if government information is exempt under this Part of the Bill, a public sector organisation is not required to provide access to the information.
Division 2 – Disclosure generally is not in the public interest

Information that falls within this division is assumed to be exempt from disclosure on public interest grounds.

The government information that falls within this Division encompasses material:

- that is produced for, or as a part of, the Cabinet and Executive Council decision-making process (clause 44(1)(a));

- sensitive information relating to decisions about the Territory’s economy (clause 44(1)(b));

- information about security and law enforcement (clause 45);

- information covered by certain secrecy provisions in other legislation (clause 46); and

- information relating to the justice system (clause 47).

Matters Confidential to Government

Clause 44(1)(a) exempts information that forms part of the decision making process of Executive bodies, i.e., Cabinet, the Executive Council and their committees. The purpose of the exemption is to preserve the confidentiality of the decision-making processes of those Executive bodies. Information is exempt under this clause:

- if it was brought into existence for submission to or consideration by an Executive body (clause 44(1)(a)(i));

- if it was brought into existence to brief a minister in relation to matters to be considered by an Executive body (clause 44(1)(a)(ii));

- if it was considered by an Executive body (clause 44(1)(a)(iii));

- if it is an agenda, minute or record of the deliberations of an Executive body (clause 44(1)(a)(iv));

- would disclose the deliberations of an Executive body (clause 44(1)(a)(v)); or

- is a draft of such information (clause 44(1)(a)(vi)).

Clause 44(1)(b) exempts information if its disclosure would seriously damage the Territory’s economy through the premature disclosure of government decisions about taxation, price controls, borrowings or trade agreements.
For the purposes of this exemption, under clause 44(2) material that is purely statistical, technical, factual or scientific information is not exempt unless its disclosure would involve the disclosure of deliberations or decisions. This exemption is further limited by clause 44(3) provides that the exemption no longer applies if 15 years has elapsed since the information came into existence.

**Security and Law Enforcement**

Clause 45 exempts from disclosure information that, if disclosed, would prejudice the security or defence of the Commonwealth or a State or a Territory and the maintenance of law and order in the Territory. Under clause 45(2) information that prejudices investigations into breaches of the law, discloses the identity of confidential information sources, discloses methods of detecting breaches of the law, facilitates escape from lawful custody or that endangers the life or physical safety of a person falls within the exemption. However, clause 45(3) limits the exemption so that information that reveals that the scope of an investigation has exceeded legal limits or has used illegal methods is not exempt.

**Secrecy Provisions**

Clause 46 exempts from disclosure information that is covered by secrecy provisions of other legislation. This exemption only applies if the secrecy provision makes it an offence to disclose the information. The provision is subject to a “sunset clause” of 5 years to enable a review of “secrecy provisions” of other legislation to be conducted.

**Preservation of system of justice**

Clause 47 exempts information that, in broad terms, relates to the system of justice. If disclosure of information would prejudice the prosecution of an offence, a person’s rights to a fair trial or would disclose information about a matter before a court or tribunal, it is exempt. Where disclosure would breach legal professional privilege or would be in contempt of parliament or a court etc., it is also exempt under this Division.

**Division 3 – Disclosure in a particular case is not in the public interest**

The thrust of clause 48 is that government information that falls within this Division is only exempt from disclosure if it is not in the public interest to disclose it. In determining the public interest, the possibility of embarrassment to or lack of confidence in the government or a public sector organisation or the possibility that information may be misunderstood are irrelevant considerations (clause 48(2)).

**Matters affecting relations with other governments**

Clause 49 exempts information from disclosure, if it is in the public interest to do so, if it would prejudice the relations between Australian or overseas governments.
**Deliberative processes**

Clause 50 exempts, subject to a public interest test, information that relates to the deliberative process of a public sector organisation. The exemption does not apply to purely statistical, technical, scientific or factual information (clause 50(2)), nor does it apply to decisions, orders or rulings made under an adjudicative function or the reasons for such a decision (clause 50(3)). Matters such as the seniority of the person involved in the deliberative process or the fact that the public may not readily understand the tentative or optional quality of the information are irrelevant to determining whether information is covered by the exemption (clause 50(4)). Under clause 50(5), the deliberative process exemption does not apply to information that is more than 10 years old.

**Internal assessment personnel matters and industrial relations**

Clause 51 covers information which, if disclosed, is reasonably likely to prejudice the effectiveness or the attainment of the objects of a test, assessment or audit conducted by a public sector organisation or which would have a substantial adverse impact on the management of employees or on the conduct of industrial relations of a public sector organisation.

**Health, safety and the environment**

Clause 52 covers information if its disclosure would prejudice measures for the protection of the health or safety of the public, harm the habitats or prejudice the protection of flora and fauna or which would prejudice the security of a prison.

**Information provided in confidence**

Clause 53 covers information provided to a public sector organisation on a confidential basis. In order to fall within the exemption, the information must have been communicated in confidence and must either be exempt if it had been originated by the public sector organisation or its disclosure would impair the ability of the organisation to obtain similar information in the future. The exemption does not cover confidential information provided under a legal requirement. The exemption applies only for five years after the information is communicated to the public sector organisation but this period can be extended by the Information Commissioner if it is in the public interest to do so for further periods up to but not exceeding five years.

**Privacy and cultural information**

Clause 54 covers information where its release would unreasonably interfere with a person’s privacy or which would disclose information about an Aboriginal sacred site or Aboriginal tradition.
Trade secrets, scientific research and examination papers

Clause 55 covers trade secrets, whether obtained by or provided to a public sector organisation or originated by a public sector organisation. The exemption also covers scientific and technical research and examination papers and associated documents. The exemption applies only for five years but the Information Commissioner can extend the period if it is in the public interest to do so. The rationale for this is that trade secrets, such as commercially valuable techniques or processes, can extend over periods longer than five years and therefore, a mechanism is required to extend the period of protection in those cases.

Financial and property interests of Territory or public sector organisations

Clause 56 exempts information if its disclosure is reasonably likely to have a substantial adverse effect on the financial or property interests of the Territory or of a public sector organisation.

Division 4 – Exemption certificates

The Bill also provides for exemption certificates. Exemption certificates establish that information is exempt because it is not in the public interest to disclose the information (clause 58). An exemption certificate is effectively a “veto” and cannot be revoked or reviewed by any appeal body (eg. the Information Commissioner or Court).

Exemption certificates are available in relation to Cabinet and Executive Council information (clause 44(1)(a)) security and law enforcement information (clause 45(l)), deliberative processes (clause 50(l)), and privacy and cultural information (clause 54). The Minister of a public sector organisation may issue an exemption for deliberative process information (clause 59(i)) and the Chief Executive Officer of the Department of the Chief Minister with respect to the remaining categories. The Minister may delegate his or her power to the relevant Chief Executive Officer but the Chief Executive Officer of the Department of the Chief Minister has no power of delegation (clause 63).

An exemption certificate lasts for two years but may be revoked earlier and may be extended where appropriate (clause 60). Exemption certificates are unreviewable and conclusively establish that information is exempt from disclosure (clause 61). An exemption certificate may not be issued once a complaint has been made to the Information Commissioner under Part 7 of the Bill (clause 62).
PART 5 – PROTECTION OF PRIVACY

Division 1 – Information Privacy Principles

Part 5 of the Information Bill imposes obligations on public sector organisations to comply with the Information Privacy Principles (IPPs), which are set out in the Schedule (clause 64). The IPPs in the Information Bill are adapted from the federal Privacy Commissioner’s National Principles for the Fair Handling of Personal Information. The National Principles were developed in consultation with business and consumer groups and government representatives. The Commonwealth’s private sector privacy legislation is also based on the National Principles. In turn, the National Principles are based on an internationally recognised benchmark developed by the Organisation for Economic Co-ordination and Development (OECD). The Northern Territory’s Information Privacy Principles will assist public sector organisations to protect the personal information that they hold.

The collection IPPs (IPP 1 and IPP 10) will not apply to personal information that was collected before the Bill comes into operation but all other IPPs will apply regardless of when the information was collected (clause 64). The phase-in period will prevent any obligations arising under the legislation until 12 months after the Bill comes into force (24 months for local authorities) (clause 158).

An “interference with privacy” occurs whenever a public sector organisation contravenes an IPP, code of practice or an authorisation (clause 66).

Division 2 – Exemptions from the IPPs

A small number of privacy-specific exemptions are contained in the Bill. These relate to publicly available information (clause 67), courts and tribunals (clause 67), law enforcement agencies (clause 67) and statistics and research (clause 70).

While publicly available information is not covered by the privacy regime, under clause 67 public registers must be kept in compliance with the IPPs to the extent that it is reasonably practicable to do so given the requirements imposed by or under an Act for keeping the register and making it available for public inspection.

There is no blanket exemption granted for law enforcement agencies but neither is it intended that the Bill interfere with the legitimate functions of law enforcement agencies. The Bill attempts to balance these interests by allowing limited departures from information-handling standards specified in the IPPs where the law enforcement agency believes on reasonable grounds that non-compliance is necessary (clause 69). “Law enforcement agency” has been defined broadly in the Bill so as to include government agencies that have legitimate law enforcement responsibilities.
Division 3 – Codes of Practice

The privacy regime provides support for self-regulatory Codes of Practice underpinned by a default legislative scheme. This ensures maximum flexibility for the Northern Territory public sector to provide appropriate protection for Territorians’ personal information. Codes of Practice are covered under this part of the Bill. Under clause 70, a public sector organisation may prepare a Code of practice. Codes allow different standards to the IPPs to be set for the collection and handling of personal information (clause 71). The Information Commissioner is required to scrutinise a prospective code and may only approve it if it substantially complies with the objects of the Bill, the organisation is capable of complying with the code and the code is not contrary to the public interest (clause 72). Once approved by the Information Commissioner, a code is submitted to the Minister who may submit the code of practice for approval to the Administrator (clause 73). The Administrator may then approve a code by notice in the Gazette (clause 74). Once this has occurred, the code of practice will have the force of law (clause 78). A code is revoked or varied in the same manner (clauses 76 and 77). The Commissioner will keep codes in a publicly available register (clause 79).

Division 4 – Authorisations

This part of the Bill provides a “safety valve” for those occasions when it may be necessary for a public sector organisation to depart from specific IPPs but it is not feasible or desirable for it to develop an entire code of practice. Instead, a public sector organisation may apply to the Information Commissioner for an authorisation to collect, use or disclose personal information in a manner that would otherwise contravene or be inconsistent with IPP 1 (collection), IPP 2 (use and disclosure) and IPP 10 (sensitive information) (clause 80(1)).

The Commissioner may only grant an authorisation if the public interest in allowing the authorisation outweighs to a significant degree the interference with privacy that might result and the benefit to persons of allowing the authorisation outweighs the interference with privacy that might result (clause 80(2)).

Division 5 – Compliance notices

This part of the Bill provides a mechanism for addressing serious contraventions of the IPPs or a code of practice. Clause 81 empowers the Information Commissioner to issue a compliance notice where a suspected breach of the IPPs or a code is “serious or flagrant” or is of a kind that has been done on at least three separate occasions within the previous two years.

A compliance notice requires the organisation to take specified action within a specified period of time to ensure that the organisation complies with the IPP(s) or code in the future (clause 81(2)). The organisation may apply to the Information Commissioner for an extension of time in order to comply with the notice (clause 82).
Non-compliance with a compliance notice will be an offence. The maximum penalty for failure to comply is $30,000 (clause 83).
PART 6 – INFORMATION COMMISSIONER

Division 1 – Establishment, functions and powers

The Bill establishes the office of the Information Commissioner, describes his or her functions and confers powers. Clause 84 provides for the appointment of the Information Commissioner. The functions of the Commissioner are very widely drawn (clause 85(1)) and include:

- the development of guidelines for public sector organisations about freedom of information and privacy;
- the promotion of the principles of freedom of information and privacy;
- the provision of advice and training to public sector organisations;
- the conduct of audits;
- the examination and assessment of proposed legislation and policies relevant to freedom of information and privacy;
- researching and monitoring developments in relation to freedom of information and privacy;
- undertaking educational programs to promote public awareness of freedom of information and privacy;
- making public statements about matters relevant to freedom of information and privacy; and
- consulting and co-operating with other persons and bodies in relation to freedom of information and the protection of privacy.

In carrying out his or her functions, the Information Commissioner must have regard to the objects of the legislation (clause 85(2)). Clause 86 confers powers on the Commissioner so that he or she may perform his or her functions under the Bill. This includes being entitled to full and free access at all reasonable times to the records of a public sector organisation and requiring a public sector organisation to answer a question or produce a record. Clause 87 requires the Information Commissioner’s staff to assist person’s to exercise their rights under the Bill but legal advice cannot be given. Clause 88 will enable the Commissioner to delegate his or her powers under the Bill in writing.
Division 2 – Appointment provisions

Clauses 89-94 are appointment provisions covering such things as the Commissioner’s terms and conditions of appointment, termination of appointment, leave of absence and resignation.

Division 3 – Miscellaneous

Under clause 95 all members of the staff of the Information Commissioner are to be employees within the meaning of the Public Sector Employment and Management Act. The Commissioner may also engage consultants (clause 95).

Clause 96 provides that the Commissioner may share staff and physical resources with another statutory officer. This may result in cost efficiencies.

The Commissioner is required to produce an annual report and may be required to report on other matters connected with the operation of the Bill (clauses 97 and 98).

Clause 100 provides that a person must not obstruct or hinder or improperly influence the Commissioner or refuse or fail to comply with a direction made by the Commissioner under the Bill (200 penalty units or imprisonment for 12 months).
PART 7 – COMPLAINTS TO INFORMATION COMMISSIONER

Division 1 – Complaints procedure

Part 7 is concerned with the resolution of complaints by the Information Commissioner. A person may complain to the Commissioner about a decision made by a public sector organisation following a request for a review of an initial FOI decision (clause 102). A person may also complain to the Commissioner about an interference with privacy (clause 103). A complaint must be made in writing (clause 104). The Commissioner has a discretion to decide not to entertain a complaint in certain circumstances. These include:

- where the time limit for making a complaint has elapsed;
- where the Commissioner does not consider that there has been an interference with privacy;
- where other complaint mechanisms have not been exhausted; or
- where the complaint is frivolous or vexatious (clause 105).

The Commissioner must give the complainant notice of whether the complaint has been accepted or not (clause 106), if accepted, and the Commissioner must also notify the respondent.

The Bill provides for the referral of complaints to the Northern Territory Ombudsman or an interstate Privacy Commissioner to ensure that complaints are resolved in the most appropriate forum (clause 107). Under clause 108, a complaint may be withdrawn at any time. Once a complaint has been withdrawn, however, it cannot be the subject of another complaint under the Bill.

If the Commissioner accepts a complaint, he or she must investigate the matter complained of (clause 109(1)). Once this investigation is completed, the Commissioner must decide whether or not a prima facie case exists (clause 109(3)). If there is insufficient evidence, the complaint must be dismissed. If there is sufficient evidence, the complaint must be referred to mediation. Mediation is the primary means by which complaints will be resolved by the Commissioner (clause 110).

If the Commissioner finds a complaint proven, he or she can make a range of orders including to order the release of government information, to order privacy breaches to cease, to order an apology for a privacy breach or to order payment of compensation for any loss or damage caused by a privacy breach (clauses 113 and 114).

The Commissioner may deal with similar complaints together (clause 116) and may discontinue the complaint when he or she is satisfied that a complainant no longer wishes to pursue a complaint (clause 117).
Division 2 – Procedure for hearings

It is only in cases where mediation fails that the complaint may be subject to final determination via a formal hearing. The procedure for a hearing is dealt with by clauses 120-127 and includes powers to compel evidence (clause 123) and a contempt provision (clause 126). Both of these provisions are subject to civil penalties in the case of non-compliance (200 penalty units or imprisonment for 12 months).

Under clause 127 the Commissioner must not conduct the hearing of a complaint if he or she has personally conducted an investigation into a complaint, has been involved in negotiations in respect of a complaint or has conducted a mediation in relation to a complaint. In cases where the Commissioner is not eligible to conduct a hearing, the Minister may appoint a person to conduct the hearing instead of the Commissioner. A person appointed to conduct a hearing is to be taken to stand in the shoes of the Commissioner and to have all the powers of the Commissioner while conducting the hearing.
PART 8 – APPEALS FROM DECISIONS OF INFORMATION COMMISSIONER

A person may appeal to the Supreme Court against a decision made by the Information Commissioner under the Bill (clause 128). Appeals to the Supreme Court will be provided on questions of law only (clause 128(2)).

On an appeal, the Supreme Court may make any of the decisions that would have been available to the Information Commissioner. For that purpose, the Court may make any orders and give any directions that the Court considers appropriate.
PART 9 – RECORD KEEPING AND RECORDS MANAGEMENT

Background

Information legislation must be underpinned by an effective record keeping and records management framework in order to:

• keep costs down;
• ensure the better management of records; and
• drive effective implementation.

The Territory has already developed a comprehensive records management framework. The Information Bill will provide legislative backing to the essential components of that records management framework.

Division 1 – Preliminary

This part of the Bill will apply to the records of all public sector organisations, including the records of a Government Business Division (clause 129(1)). It will not apply to the records of a court or tribunal in respect of a proceeding or other matter before the court or tribunal (clause 129(2)). The chief executive officer of each public sector organisation will be responsible for ensuring that the organisation complies with this part of the Bill (clause 130).

Division 2 – Obligations of public sector organisations

The framework includes:

• the need to protect records (clause 132);
• to make and keep accurate records of government activities (clause 133(a));
• to establish and maintain a records management system (clause 133(b));
• to monitor and report on the system (clause 133(c)); and
• to keep technology-dependent records accessible (clause 134).

The purpose of ensuring that full and accurate records of all Northern Territory Government business transactions are created and maintained in a records management system is to demonstrate accountability for those transactions and to ensure that full evidence of the transactions is upheld. Clause 134 recognises that an essential element of records management relates to the ability of the records to be used
and accessed over time. Increasingly, electronic records are being generated by organisations – it is critical that electronic records are capable of being read and reproduced over time, given the high degree of redundancy of information technology systems and software.

**Division 3 – Standards**

The Northern Territory Archives Services (NTAS) will be assigned the responsibility of overseeing the record-keeping component of the Information Bill. NTAS has the expertise to ensure that the Northern Territory Government’s records management framework is coordinated and capable of supporting the objects of the Information Bill (clause 131). NTAS will be given the role of preparing standards for managing records (clause 135(1)). Standards cover a wide range of matters under clause 135(2), and the sub-clause is not exhaustive. Standards will provide an important compliance tool for agencies. The standards prepared by NTAS will provide detailed instructions on such issues as: what is a record? What is an archive? When can records be destroyed? Clause 136 provides that the Minister may approve standards by notice in the *Gazette*.

Clause 137 provides that NTAS must review a standard at least once every three years. NTAS must also provide public sector organisations with assistance in order to enable the organisation to comply with any standards applicable to the organisation (clause 138).

**Division 4 – Archiving records**

The Bill also provides for the archiving of Northern Territory records including dealing with:

- the classification of archives (clause 140);
- access to open archives (clause 141);
- access to closed archives (clause 142); and
- accessing or correcting archives not yet publicly available (clause 143).

**Division 5 – Offence**

An offence of mishandling records is created by clause 144 (200 penalty units or imprisonment for 12 months). This clause prescribes an offence for mishandling records under this part of the Bill. Mishandling records includes abandoning, deleting or disposing of a record or damaging or altering a record.

These actions would be judged according to the standards established by the archives service. For example, it does not mean that records cannot be destroyed, merely that
records that are classified as evidence of government activity cannot be destroyed outside of the terms of the disposal standard developed by the archives service.

There are two further defences to this offence. If a defendant demonstrates that he or she was acting in the course of his or her employment or did not or could not reasonably have known that he or she was dealing with a record, then the defendant has not committed an offence under this part of the Act.
PART 10 – GENERAL OFFENCES AND MATTERS RELATING TO LIABILITY

Division 1 – General offences and related procedural matters

Part 10 outlines a number of general offences and matters relating to liability. Clause 145 provides that it is an offence for a person to make false or misleading statements in relation to the information regime established by the Information Bill (100 penalty units or imprisonment for 6 months). Clause 146 provides that it is an offence to conceal or dispose of government information in order to prevent access or correction under the information regime (100 penalty units or imprisonment for 6 months). Clause 147 is a confidentiality provision that prohibits public sector organisations and the Information Commissioner and his or her staff from disclosing information gained in the course of the performance of their functions (2,500 penalty units or imprisonment for 2 years).

Clause 148 ensures that outsourcing arrangements are covered by the privacy regime established by the Information Bill. It is intended that providers of contracted services will be bound under the Bill to the same extent as the public sector organisation seeking to outsource one or more functions. The level of obligation will either be according to the default legislative scheme (the IPPs), an approved code of practice or an authorisation and is linked to acts or practices undertaken for the purposes of a service contract.

This policy is achieved by allocation of responsibility for any contraventions of the Bill, 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-clauses (3) (c) and (d). The first is that a suitable service 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, code or authorisation must be enforceable against the contracted service provider within the Northern Territory’s jurisdiction. The purpose of this clause is to ensure that individuals whose personal information is misused outside the Northern Territory retain a practical means to address contraventions. If data handling obligations are not specified in a service contract the outsourcing organisation would be responsible according to the Bill or the extent specified in a code or authorisation.

Clause 149 provides that if it is necessary to establish the state of mind of a person or body corporate in the prosecution of an offence under the Bill, it is sufficient to show that the conduct was engaged in by a director, employee or agent of a body corporate or an employee or agent of a natural person within the scope of his or her actual or apparent authority and that the director, employee or agent had that state of mind.
Division 2 – Legal immunity

Clauses 150, 151 and 152 provide immunity from liability under certain circumstances including where a person exercises a power, performs a function or complies with a requirement under the Bill; as a result of making an application under the Bill; and where a public sector organisation has granted access to government information, including personal information, voluntarily but where the organisation would have been required to provide that access had an application been made under the Bill. This final provision is designed to support the pro-disclosure approach of the Bill.
PART 11 – MISCELLANEOUS

This point assembles miscellaneous provisions necessary for the operation of the Bill. Clause 153 provides that no review or proceedings exist except as provided for by the Information Bill. Clause 154 outlines how applications and complaints may be made by or on behalf of children, persons with impairments or deceased persons. In the case of deceased persons a five-year time period applies.

Clause 155 provides for fees for applications and complaints to be dealt with by the regulations.

Clause 156 deals with the situation where a public sector organisation ceases to exist or becomes defunct. If the organisation’s functions are taken over by another public sector organisation, that organisation also takes on any outstanding responsibilities under the Information Bill. If the functions are not taken over, then a public sector organisation nominated by the relevant Minister will take on any outstanding responsibilities. This ensures that no gaps arise under the information regime.

Clause 157 provides that the Administrator may make regulations, not inconsistent with the Bill, in order to enable the Bill to work properly and effectively.

Clause 158 outlines the proposed application of the legislation. It is envisaged that the new information regime will commence on 1 July 2002. However, public sector organisations will have a twelve-month phase-in period before the FOI regime or the Information Privacy Principles or a code of practice will be enforceable. This will allow public sector organisations time to review their systems, to exhaust stationery supplies and to put new procedures in place to ensure they comply with the new legislation. Local Government has been granted an extended phase-in period of twenty-four months in order to allow adequate time for compliance initiatives to be developed. During this time the Information Commissioner will commence community and public sector education campaigns, provide compliance advice and register codes of practice.

Clause 159 provides that the Northern Territory Attorney-General’s Department must review the information regime established by the Information Bill five years after it commences operation. This is designed to ensure that the Bill is working smoothly and efficiently and is giving effect to the objects of the Bill.
SCHEDULE – INFORMATION PRIVACY PRINCIPLES (IPPs)

IPP 1 – Collection

This principle sets out a framework for the collection of personal information. It includes requirements that public sector organisations only collect personal information if it is necessary and it must be collected by lawful and fair means and not in an unreasonably intrusive way. Additional collection requirements apply where sensitive information is being collected (IPP 10).

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.

Wherever possible, public sector organisations must collect information directly from the individual. If this is not possible, the organisation must take reasonable steps to ensure that the individual is aware of the collection.

IPP 2 – Use and disclosure

This principle governs the use and disclosure of information held by organisations. In general, public sector 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, public sector organisations 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. In the case of sensitive information, the use or disclosure must be directly related to the primary purpose of collection.

Further secondary uses and disclosures are otherwise permitted on public interest grounds. These include, for example, where there is a serious threat to life or where disclosure is required by law.

IPP 3 – Data quality

This principle is a quality assurance principle that seeks to ensure that personal information collected, used and disclosed by a public sector organisation is accurate, complete and up to date.

IPP 4 – Data security

This principle requires public sector organisations to protect the security of personal information they hold, ensuring that there is no misuse, loss, unauthorised access,
modification or disclosure of the information. Organisations are also required to take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed for any purpose.

IPP 5 – Openness

This principle encourages transparency by requiring public sector organisations to document clearly their policies for the management of personal information and to make those policies available to the public.

Public sector 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.

IPP 6 – Access and correction

This principle provides individuals with a right to access their personal information and to request corrections to it where necessary

If access is not permitted because of an exemption (for example, access poses a serious or imminent threat to the life or health of an individual), the public sector organisation is still required to consider whether the use of an intermediary would be adequate to satisfy a request for access. This principle is complementary to the access and correction rights outlined in the Information Bill.

IPP 7 – Unique identifiers

This principle imposes limits on the use of unique identifiers by and between public sector organisations. Unique identifiers must be necessary to enable the organisation to perform its functions efficiently and they cannot be shared between organisations unless it is necessary to enable the organisation to perform its functions efficiently, the individual consents or it is required under an outsourcing arrangement.

IPP 8 – Anonymity

This principle provides that, wherever it is lawful and practicable, individuals have a right to remain anonymous when dealing with public sector organisations.

IPP 9 – Transborder data flows

This principle puts limits on the flow of personal information outside of the Northern Territory. An organisation is only allowed to transfer personal information outside the Northern Territory if it reasonably believes the recipient is subject to a law, or other binding obligation, that requires compliance with a privacy framework that is
substantially similar to the IPPs. Personal information may also be transferred where
the individual consents; it is necessary for the performance of a contract; or the transfer
is for the benefit of the individual, it is not practicable to obtain the individual's consent
and it is likely that the individual would consent to the transfer.

**IPP 10 – Sensitive information**

This principle provides more stringent requirements for the collection of sensitive
information. These are in addition to the requirements outlined in IPP 1.

Sensitive information means personal information about an individual's racial or ethnic
origin, political opinions, membership of a political, professional or trade association or
trade union, philosophical or religious beliefs or affiliations, sexual preferences or
practices, criminal record or health information.

A public sector organisation cannot collect sensitive information unless: the individual
consents; it is required by law; the individual is physically or legally incapacitated; or the
collection is necessary to establish, exercise or defend a legal or equitable claim.

In very limited circumstances, sensitive information can be collected without consent in
relation to government funded welfare or educational services.