REPORT

Sharing of Personal Information in the Event of Disasters inside or out of the Northern Territory

CONSULTATION OUTCOMES

April 2014

Legal Policy
Department of the Attorney-General and Justice
68 The Esplanade, Darwin NT 0800
GPO Box 1722, DARWIN NT 0801
File 20121571; PCD14/2261
Telephone: (08) 8935 7659 Facsimile: (08) 89357662
http://www.nt.gov.au/justice

This Page Intentionally left blank.

Table of Contents

1. RECOMMENDATIONS

Proposal number (and paragraph in the report)	Details of the proposal
5.1.3	Section 70 of the *Information Act* be amended so that it applies to NT Emergency Services and NT Fire and Rescue Services as well as to law enforcement agencies
5.2.3	IPP 2.1(d)(iii) in Schedule 2 of the *Information Act* be amended to include the words "public welfare" and that the term be defined so that it links with the definition of "emergency situation" under the *Emergency Management Act*
5.3.3	The *Information Act* be amended to insert a provision that provides that: • "permitted purpose" be defined in similar terms as clause 5(1), 5(2)(a), 5(2)(b), 5(2)(c) and 5(2)(d) of the New Zealand Civil Defence National Emergencies (Information Sharing) Code 2013 • a public sector organisation may use, collect or disclose personal information within or outside of the Northern Territory for a permitted purpose during an "emergency situation" as defined in the *Emergency Management Act*; and • a public sector organisation may apply to the Information Commissioner in writing for an extension of the period of time after the "emergency situation" has ceased to use, collect or disclose personal information for a permitted purpose.
5.4.3	The endpoint of an emergency be determined based on a legislative approach where the period of exemption is defined by a link to an event such as the declaration of an "emergency situation" in the *Emergency Management Act*
5.5.3	(a) Division 3 of Part 5 of the *Information Act* be amended to provide that Codes of Practice are made when approved by the Information Commissioner; and (b) Section 81(1) of the *Information Act* be amended to extend the scope of Grants of Authorization to all IPPs.

2. INTRODUCTION

2.1 Background to the release of the Issues Paper

Public sector organisations hold large amounts of personal information about members of the public. In an emergency situation, it may be essential for one of these organisations to assist an emergency body, public sector organisation or public officer trying to take necessary action to provide aid, relief, rescue or recovery assistance.

The Information Commissioner, Ms Brenda Monaghan, has in the past raised concerns with the Department of the Attorney-General and Justice that the privacy provisions in the *Information Act* may not be sufficiently flexible to permit the sharing of essential information in the event of a disaster or emergency situation in the Northern Territory. In particular, there is concern that the Act may not adequately provide power for public sector organisations to share information following a disaster after the immediate threat has subsided, but aftermath and recovery of the disaster still demands high levels of co-operation between agencies.

In developing the Issues Paper, the Information Commissioner suggested the need for any proposals to be assessed against policy goals. The proposed policy goals are as follows:

- aim to provide **certainty**. It would need to be clear to public sector employees when an applicable emergency situation is occurring, and what kind of information sharing is permitted during that period of time. It would be undesirable for organisations to fail to meet emergency needs or provide basic services because they are uncertain that they are able to provide information;
- is adequately **flexible**. It recognises that some disasters will have little or a temporary impact on information systems, whereas others could potentially involve complete system failure. The length of time the exemption is needed could vary, and it is possible for disasters to move geographically over a period of time;
- have a **mechanism to restore adherence to the Information Privacy Principles.** The Office of the Information Commissioner's enquiries have indicated that once systems are opened and practices change during an emergency information-sharing episode, it requires a conscious decision and effort to change them back. Something must trigger this decision or convenience and curiosity may encourage organisations to simply keep sharing;
- **limit privacy risks** by departing from the IPPs only to the extent justifiable in the public interest. The Information Commissioner suggests that the IPPs represent best practice in most situations, and hence should be modified to the minimum extent necessary to achieve the objectives of the exemption; and
- **not unduly onerous.** The application of the exemption should not require some extraordinary amount of paperwork or the presentation of expert evidence.

There are three kinds of emergency factual scenarios:

(i) a 'state of emergency' type disaster where central government infrastructure is lost (eg a cyclone destroying many Darwin buildings, the Christchurch earthquake);

(ii) a localised emergency which may interrupt or damage information systems (eg flooding in a community or a series of communities); and

(iii) a disaster which occurs outside the jurisdiction (eg the Bali bombings or a tsunami in a tourist area).

The Information Commissioner originally raised only the first kind of scenario as a situation that requires this kind of exemption. The difficulty noted in other

jurisdictions has been that this kind of significant disaster at home leaves people without much ability to create a Code of Conduct or other such agreement under the *Information Act* to permit information sharing that would otherwise be in breach of the IPPs. A localised emergency would not create this same degree of chaos, however localised emergencies may require an urgent information sharing response by persons caught up in the local emergency, particularly given the geographically remote nature of many communities in the Territory.

The third situation (occurring outside of the NT or Australia), however, raises a host of complex policy questions about the security of the personal information being transferred. The public interest in, say, identifying bodies, must be balanced against the dangers of disclosing biometric data to jurisdictions where such information may leak or be abused. Individuals cannot modify their biometric data if it is compromised, and any weighing of public policy considerations must include that 'lifetime risk'. This includes an appreciation that technology is sufficiently advanced, making it likely that reliance on biometric data will become more common in the near future, and that identity theft is an increasing international issue. Another point of distinction is that in this kind of emergency, highly competent teams are created to perform dedicated functions such as body identification, and are in a good position to put together a Code of Conduct proposal. Previous teams have managed, for example, to individually contact large numbers of families to seek consent to the transfer of biometric data for identification purposes outside the jurisdiction.

The impact of a disaster generally and the need for information sharing may only be loosely related. A severe disaster might have only a minor impact on information systems, and a relatively localised disaster could destroy systems that may be hard to replace. Hence, a provision should be designed to be flexible enough to cater for the following situations:

- disaster has no impact on information systems and there is no good reason to permit departure from the IPPs;
- disaster has a temporary impact – for example, a widespread loss of power may result in a temporary inability to retrieve information from usual systems which ends as soon as the power is restored, which may occur before the disaster period is over;
- disaster has a long-term impact which extends after the initial 'disaster period' – for example, if the NT Government servers were physically destroyed, it could take months or years to recover systems and data, and workarounds might be justifiable for some time; and
- disaster creates a need for additional information use – for example, to contact persons following the event to coordinate the provision of services.

2.2 Release of the Issues Paper

An Issues Paper, titled "*Sharing of Personal Information in the event of Disasters inside or out of the Northern Territory*", was released in July 2013. It was published via the Department of the Attorney-General and Justice website. Additionally, letters were sent to stakeholders and interested bodies informing them of the release of the Issues Paper.

The Paper sought comments from various stakeholders and the general public on proposed amendments to the *Information Act* to establish a clear legal basis for the collection, use and disclosure of personal information in the event of a disaster or an emergency that might occur inside or outside of the Territory. The issues paper was prepared in consultation with the Information Commissioner.

Submissions on the Issues Paper closed in September 2013.

2.3 Stakeholder consultations following release of the Issues Paper

Submissions were received from the following stakeholders:

- Information Commissioner;
- Registrar-General/Public Trustee; and
- Northern Territory Police, Fire and Emergency Services.

3 SUBMISSIONS ON REFORM OPTIONS

Stakeholders were generally supportive of the proposed amendments. It was also identified that in addition to the NT Emergency Services, the NT Fire and Rescue Services was another public sector organisation that should be included for the purposes of section 70 of the *Information Act*. Concerns were also raised regarding having multiple pieces of legislation dealing with emergencies and disasters.

Comments were also made with regard the *Disasters Act* and the Commonwealth Government's review of the *Privacy Act 1988 (Cth)* and Australian Privacy Principles at the time.

On 27 November 2013, the *Emergency Management Act 2013* was enacted. That Act, among other things, repealed the *Disasters Act* and introduced a new category of emergency events referred to as "emergency situation". The enactment of this legislation has been taken into account in preparing this report.

On 12 March 2014, the Commonwealth Government enacted changes to the *Privacy Act 1988 (Cth)* including introducing a new set of Australian Privacy Principles. The comments relating to the legislative changes made by the Commonwealth Government have not been progressed as they are beyond the scope of this Report.

4 BACKGROUND OUTLINE OF THE LEGISLATION

The IPPs, set out in Schedule 2 of the *Information Act*, establish the rules for the reasonable handling of personal information by public sector organisations (refer Appendix A). They provide for the exchange of some information in emergency situations. It is not clear that they permit the large exchange of necessary information in all emergency situations.

4.1 Current Provisions of the *Information Act* that dis-apply the IPPs

There are limited exceptions in the *Information Act* that provide for the non-application of the IPPs.

4.1.1 Section 70

Section 70 of the *Information Act* provides that a law enforcement agency is not required to comply with an IPP if it believes that non-compliance is necessary for one of its law enforcement functions. These functions include (but are not limited to) locating missing persons and next of kin and providing services in emergency and disaster situations.

A 'law enforcement agency' is defined in section 4 of the *Information Act* and includes the Police Force of the Northern Territory; the police force of the Commonwealth or of a State or another Territory of the Commonwealth; or the Australian Crime Commission. It also includes a body established under a law of the Territory, of the Commonwealth, or of a State or another Territory of the Commonwealth, that performs one or more of the following functions:

- 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 or the enforcement of such a law or of a decision, direction, order or other requirement under such a law;
- protecting public revenue; or
- executing or implementing a decision, direction, order or other requirement of a court or tribunal, including executing warrants.

4.1.2 Secondary purposes

IPP 2.1 prohibits the use or disclosure of personal information about an individual for a purpose other than the primary purpose for collecting it. However, sensitive information can be used or disclosed for a secondary purpose if the secondary purpose is directly related to the primary purpose for collecting the information and the individual would reasonably expect the organisation to use or disclose that information for the secondary purpose. In addition, non-sensitive information can be used or disclosed for a secondary purpose if the secondary purpose is related to the primary purpose for collecting the information and the individual would reasonably expect the organisation to use or disclose that information for the secondary purpose.

IPP 2.1(d) also permits use or disclosure for a secondary purpose if the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to the individual's or another individual's life, health or safety; or

(ii) a serious or imminent threat of harm to, or exploitation of, a child; or

(iii) a serious threat to public health or public safety.

Furthermore, IPP 2.1(f) permits use or disclosure for a secondary purpose if it is required or authorised by law.

4.1.3 Codes of Practice and Grants of Authorisation

Part 5, Division 3 of the *Information Act* provides for Codes of Practice and Part 5, Division 4 provides for Grants of Authorisation, which permit organisations to depart from the IPPs in certain limited circumstances.

This existing mechanism should not be overlooked as a tool to deal with post-emergency information sharing. However, in the event of a state of emergency type disaster, it would be difficult and impractical to develop a Code of Practice or a Grant of Authorisation straight away, but it may be that these solutions are better for more long-term information sharing needs that arise following a disaster.

5 OPTIONS CONSIDERED

5.1 Section 70 of the *Information Act* be amended so that it applies to NT Emergency Services as well as to law enforcement agencies

5.1.1 Submissions

The Northern Territory Police, Fire and Emergency Services (NTPFES) supported the inclusion of the Northern Territory Emergency Services to the application of section 70 of the *Information Act*. However, NTPFES identified a need to ensure that the proposal assisted other public sector organisations such as the Northern Territory Fire and Rescue Services in exchanging personal information in emergency situations (eg information sharing between the Department of Health and NTPFES where casualties are extracted from disaster scenes) where quick time exchange may be vital in managing risks and disaster responses.

The Information Commissioner and the Registrar-General/Public Trustee supported the proposal.

5.1.2 Discussion

The policy intent of the proposal is that section 70 of the *Information Act* applies to all public sector organisations involved in responding to emergency or disaster situations, if the organisation believes on reasonable grounds that not complying with any IPP including IPP 2 (on the use and disclosure of personal information) is necessary for one or more of its functions. This would include the Northern Territory Fire and Rescue Services.

5.1.3 Proposal

Section 70 of the *Information Act* be amended so that it applies to NT Emergency Services and NT Fire and Rescue Services as well as to law enforcement agencies.

5.2 IPP 2.1(d)(iii) in Schedule 2 of the *Information Act* be amended to include the words "public welfare" and that the term be defined so that it includes emergency situations

5.2.1 Submissions

NTPFES did not support this proposal citing that the Issues Paper notes that the proposed amendment would result in an impractical impost on emergency services in complying with different pieces of legislation.

In addition, NTPFES noted that, as currently worded, IPP 2.1(d)(i) and (ii) created a limitation to the use or disclosure of personal information due to the words "imminent threat", which suggested that use or disclosure could only occur prior to the threat materialising. NTPFES queried if there was a proposal to amend this limitation.

The Information Commissioner and the Registrar-General/Public Trustee supported the proposal.

5.2.2 Discussion

IPP 2.1 prohibits the use or disclosure of personal information about an individual for a purpose other than the primary purpose for collecting it unless the use or disclosure falls into one of the exempt circumstances it provides (refer to paragraph 4.1.2 of this Report). Currently, the wording of IPP 2.1(d) does not allow for the use or disclosure of personal information for a secondary purpose in the event of an emergency or disaster. As such, it is necessary that IPP 2.1 is amended to include this additional exemption.

Under the *Information Privacy Act 2000* (Vic), IPP 2.1(d) uses the same words as the NT IPP 2.1(d) but includes the words "public welfare". Arguably, the use of the term "public welfare" in this context includes offering assistance to victims and assisting the community to more generally overcome the effects of disasters and other trauma. A definition of "public welfare" will also ensure that unintended information sharing does not occur as it will be clear in what circumstances personal information can be used or disclosed.

The words "serious and imminent threat" in IPP 2.1(d)(i) and (ii) relate to a threat to an individual's life, health or safety or threat of harm to or exploitation of a child. The words have a specific meaning in the context. Any amendment to these principles would derogate from their original intention, that is, to lessen or prevent a serious and imminent threat prior to that threat materialising. As such, no change to these principles is proposed.

On 27 November 2013, the *Emergency Management Act 2013* was enacted. That Act, among other things, repealed the *Disasters Act* and introduced a new category of emergency events referred to as "emergency situation" and rationalised the definitions of "state of emergency" and "state of disaster".

The comments in the Issues Paper relating to public sector organisations not having time resources to comply with different legislative instruments or common law were made in reference to IPP 2.1(f) rather than in reference to IPP 2.1(d). IPP 2.1(f) provides that a public sector organisation must not disclose personal information

about an individual for a secondary purpose unless "the use or disclosure is required or authorised by law". It is appropriate that IPP 2.1(f) is as broad as currently provided for as it is not possible to comprehensively list all the possible requirements or authorisations under law for the use or disclosure of personal information.

5.2.3 Proposal

IPP 2.1(d)(iii) in Schedule 2 of the *Information Act* be amended to include the words "public welfare" and that the term be defined so that it links with the definition of "emergency situation" under the *Emergency Management Act*.

5.3 The *Information Act* be amended to insert a provision that provides that:

- **a public sector organisation may use, collect or disclose personal information within or outside of the Northern Territory for a permitted purpose during a disaster or emergency or within a period of 28 days following the disaster or emergency (with the factual existence of a disaster or emergency being determined by reference to decisions made under the relevant legislation that deals with disasters and emergencies);**
- **a public sector organisation may apply to the Commissioner in writing for an extension of the period of time beyond the 28 days described above to use, collect or disclose personal information for a permitted purpose; and**
- **"permitted purpose" be defined in similar terms as section 5(1), 5(2)(a), 5(2)(b), 5(2)(c) and 5(2)(d) of the New Zealand Code.**

5.3.1 Submissions

NTPFES did not object to the proposal. However, NTPFES noted that the Issues Paper identified two possible definitions of "a disaster or emergency" – a broad generic definition or a narrow and descriptive definition. The Issues Paper noted that a broad definition not linked to an external definition based in the *Disasters Act* would become a matter of individual discretion as to whether a situation constituted a disaster or emergency. This uncertainty could be ameliorated by making the definition of emergency or disaster as descriptive as possible. NTPFES queried which proposal for the definition of "a disaster or emergency" was preferred.

The Information Commissioner and the Registrar-General/Public Trustee supported the proposal.

5.3.2 Discussion

The proposal would eliminate uncertainty surrounding the lawful exchange of personal information from public sector organisations in an emergency or disaster within or outside the Territory. The proposal does not differentiate between sensitive and non-sensitive information and the same discretion to use, collect or disclose information applies to both sensitive information and non-sensitive information. The *Information Act* defines "sensitive information" to include matters such as sexual preferences or practices, criminal record and health information.

There is strong argument that even in an emergency or disaster situation, public sector organisations should treat sensitive information with a higher level of scrutiny

that non-sensitive information. The risk of abuse or inadvertent privacy invasions is reduced by adopting a prescriptive approach to creating boundaries for use, collection or disclosure of personal information.

The New Zealand Civil Defence National Emergencies (Information Sharing) Code 2013 has a highly prescriptive approach to establishing parameters within which personal information can be used, collected or disclosed in an emergency. Clause 5 of the New Zealand Code establishes "permitted purposes" that includes matters such as identifying individuals, assisting individuals to obtain repatriation or medical services and coordination and management of an emergency. Clause 5 of the New Zealand Code reads:

5 Meaning of permitted purpose

(1) A **permitted purpose** is a purpose that directly relates to the government or local government management of response to, and recovery from, an emergency in relation to which a state of national emergency exists.

(2) Without limiting subclause (1), any of the following is a **permitted purpose** in relation to an emergency:

(a) identifying individuals who:

(i) are or may be injured, missing or dead as a result of the emergency;

(ii) are or may be otherwise involved in the emergency;

(b) assisting individuals involved in the emergency to obtain services such as repatriation services, medical or other treatment, health services, financial and other humanitarian assistance;

(c) assisting with law enforcement in relation to the emergency;

(d) coordination and management of the emergency;

(e) ensuring that people who are **responsible** for individuals who are, or may be, involved in the emergency are appropriately informed of matters that are relevant to:

(i) the involvement of those individuals in the emergency; or

(ii) the response to the emergency in relation to those individuals.

(3) For the purposes of subclause (2), a person is **responsible** for an individual if the person is:

(a) a parent of the individual;
(b) a child or sibling of the individual and at least 18 years old;
(c) a spouse, civil union partner or de facto partner of the individual;
(d) a relative of the individual, at least 18 years old and a member of the individual's household;
(e) a guardian of the individual;
(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

The comments relating to the definition of "a disaster or emergency" in the Issues Paper were made in the context of the then proposed amendments to the *Disasters Act*. As mentioned earlier, the E*mergency Management Act 2013*, among other things, repealed the *Disasters Act* and introduced a new category of emergency events referred to as "emergency situation".

The Issues Paper concluded that a descriptive definition of "a disaster or emergency" was the preferred proposal. Indeed, the Paper stated:

"A linked exemption is clearly justifiable and has the advantage of simplicity, rather than a need to apply multiple legislative tests".

Of note, at the time of drafting the Issues Paper, the Information Commissioner preferred an exemption linked to the *Disasters Act* rather than a separate test under the *Information Act*.

"Emergency situation" is defined in section 18 of the *Emergency Management Act 2013* to include declarations made by the Minister for Police, Fire and Emergency including declarations of a state of disaster or a state of emergency as well as the time a tropical cyclone watch or warning is issued for an area by the Bureaus of Meteorology. The "emergency situation" lasts until the Minister declares that it no longer exists. In the case of a tropical cyclone watch or warning, the "emergency situation" lasts until the end of the 3rd day after the watch or warning is issued or the Minister declares that the emergency situation no longer exists, whichever is earlier. To this end, any definition of "a disaster or emergency" will be linked to the *Emergency Management Act*.

Initially, it was proposed that information would be used, collected or disclosed during the disaster or emergency or within a period of 28 days following the disaster or emergency. However, as mentioned above, the *Emergency Management Act* now provides a definition of the time period of an "emergency situation".

Most "emergency situations" are not time limited (except in the case of a tropical cyclone watch or warning) and can stay in force until cancelled by the Minister upon the completion of a recovery phase. If related information sharing was needed after the "emergency situation" had ended, the amendment should allow for an application to the Information Commissioner to extend the post-emergency information sharing for a period of time. The application process would provide sufficient scrutiny that the sharing of the information after the "emergency situation" has come to an end is necessary and required.

5.3.3 Proposal

The *Information Act* be amended to insert a provision that provides that:

- "permitted purpose" be defined in similar terms as clause 5(1), 5(2)(a), 5(2)(b), 5(2)(c) and 5(2)(d) of the New Zealand Civil Defence National Emergencies (Information Sharing) Code 2013;
- a public sector organisation may use, collect or disclose personal information within or outside of the Northern Territory for a permitted purpose during an "emergency situation" as defined in the *Emergency Management Act*; and
- a public sector organisation may apply to the Information Commissioner in writing for an extension of the period of time after the "emergency situation" has ceased to use, collect or disclose personal information for a permitted purpose.

5.4 The endpoint of an emergency be determined based on a legislative approach where the period of exemption is defined by a link to an event such as the declaration of an 'Emergency Situation' in the *Disasters Act*

5.4.1 Submissions

The Information Commissioner and the Registrar-General/Public Trustee supported the proposal. NTPFES did not make any submission on this issue.

5.4.2 Discussion

A clear time period for the suspension of the prohibition in the IPPs of the use or disclosure of personal information is required to ensure that a return to the IPPs is implemented when the disaster or emergency is over.

As mentioned earlier, the *Emergency Management Act 2013*, among other things, repealed the *Disasters Act* and introduced a new category of emergency events referred to as an "emergency situation".

5.4.3 Proposal

The endpoint of an emergency be determined based on a legislative approach where the period of exemption is defined by a link to an event such as the declaration of an "emergency situation" in the *Emergency Management Act*.

5.5 Codes of practice should be made by either the Minister or the Information Commissioner and that grants of authorization cover all IPPs

5.5.1 Submissions

The Information Commissioner did not support the proposal to allow Ministers to independently issue a Code of Practice for their own Department without consultation and approval by the Commissioner. The Information Commissioner asserted that the Commissioner acts as a safeguard of both privacy and transparency and should have a role in scrutinising, commenting on and approving Codes of Practice.

The Registrar-General/Public Trustee supported the proposal. NTPFES did not make any submission on this issue.

5.5.2 Discussion

The Information Commissioner has noted that the current mechanisms for developing a Code of Practice are onerous and could be simplified. Currently, a Code is drafted by a public sector organisation, which then submits the draft Code to the Information Commissioner for recommendation to the Minister on behalf of the Department seeking the Code. The Minister submits the draft Code to the Administrator for approval and gazettal. Of note, the Minister must not put forward a Code for approval by the Administrator unless, among other things, the Information Commissioner has recommended its submission.

The Information Commissioner supports a simpler procedure whereby application is made by an organisation to the Commissioner and the Commissioner grants approval, and publishes the Code on its website. The Department that is seeking

approval of the Code presumably is working in line with its Minister's vision. The Information Commissioner opined that it is difficult to see what the extra steps accomplish except for a lot of red tape.

Given that the Information Commissioner is involved in the development and recommendation of the Codes of Practice, and especially the fact that, currently, a Code cannot be submitted for the Administrator's approval unless the Commissioner recommends so, granting of approval should be the role of the Commissioner. This is the case with Grants of Authorisations which are granted only by the Commissioner.

The Issues Paper noted that, if it is considered that the Executive Government should have a role in approving Codes of Practice, it is probably sufficient that the Minister responsible for the privacy provisions of the *Information Act* should have the role. However, to maintain the current role of the Information Commissioner in the approval process, it would require that the Minister must only approve a Code of Practice if the Commissioner has recommended so.

To also give the Minister the power to approve Codes of Practice will create two processes for approval. The Ministerial process may diminish efficiency gains advanced by the policy intent to reduce red tape for the approval of Codes, as organisations will still need to take the further step of seeking Ministerial approval following the Commissioner's recommendations. It may well be that organisations will, if given the choice between seeking approval from the Commissioner or from the Minister, choose the Commissioner's approval process as it would arguably involve lesser time and resources. As such, it is not proposed that the Minister also have the power to approve Codes.

With respect to Grants of Authorisation, the Information Commissioner notes that these only allow exemptions for IPPs 1, 2, and 10. This may be insufficient in a disaster, where IPPs involving data security, integrity, and cross-border information flow may also pose problems. There is no clear rationale for restricting Grants of Authorisation to IPPs 1, 2, and 10. The Information Commissioner has indicated support for extending the scope of Grants of Authorisation to all IPPs.

5.5.3 Proposal

(a) Division 3 of Part 5 of the *Information Act* be amended to provide that Codes of Practice are made when approved by the Information Commissioner; and

(b) Section 81(1) of the *Information Act* be amended to extend the scope of Grants of Authorization to all IPPs.

6 OTHER ISSUES

NTPFES, in its submission of September 2013, noted that the Office of the Australian Information Commissioner was proposing amendments to the *Privacy Act 1988* (Cth) and the Australian Privacy Principles. NTPFES suggested that it would be worth considering that a consistent approach is taken between Commonwealth and

Northern Territory legislation to ensure legislative principles are applied equally across jurisdictions.

The Commonwealth Government enacted those changes on 12 March 2014. It is too soon afterwards to consider the implications of those changes to the Northern Territory *Information Act* and Information Privacy Principles. It may also take some time for the Commonwealth Government to fully implement those changes, for their implications to be felt by the general community and before there is substantial data to analyse the effectiveness of those changes.

It is worth noting that the Northern Territory *Information Act* and the Information Privacy Principles are based on the Commonwealth's National Privacy Principles, which have now been replaced by the Australian Privacy Principles. However, the National Privacy Principles continue to apply to acts that occurred before 12 March 2014.

Formulating a consistent approach between Commonwealth and Territory information legislation is beyond the current policy scope of this Report.