ISSUES PAPER:

SHARING OF PERSONAL INFORMATION IN THE EVENT OF DISASTERS INSIDE OR OUT OF THE NORTHERN TERRITORY

Legal Policy Division
Department of the Attorney-General and Justice
68 The Esplanade, DARWIN NT 0800
GPO Box 1722, DARWIN NT 0801
Telephone: (08) 8935 7657 Facsimile: (08) 8935 7662
http://www.nt.gov.au/justice/

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 Introduction

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, wrote to the Chief Executive Officer of the then Department of Justice, Mr Greg Shanahan, on 2 April 2012 to express concern 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. A previous letter from the Information Commissioner raising this issue was sent to the Chief Executive Officer of Justice in July 2009. The decision was made at that time to defer consideration of the issue until the *Information Act* review. For various reasons, that review has not been completed.

The Information Commissioner's view was that the *Information 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.

The Information Commissioner stated it would be prudent to amend 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. The Commissioner only raised issues concerning disasters that might occur in the NT. This issues paper also deals with disasters that may have occurred outside of the NT and which may involve persons with a NT connexion.

This issues paper has been prepared in consultation with the Information Commissioner.

2 Consultation

You are invited to provide comments on this issues paper to the Department of the Attorney-General and Justice. Comments can be as short or informal as an email or letter, or it can be a more substantial document. Comments do not have to address all aspects of this Issues Paper. Electronic copies should be sent whenever possible.

Comments should be sent to:

Director, Legal Policy
Department of the Attorney-General and Justice
GPO Box 1722,
DARWIN NT 0801

Or by email to Policy.AGD@nt.gov.au

The closing date for comments on this draft review is 30 September 2013.

Any feedback or comment received by the Department of the Attorney-General and Justice will be treated as a public document unless clearly marked as 'confidential'. In the absence of such clear indication, the Department of the Attorney-General and Justice will treat the feedback or comment as non-confidential.

Non-confidential feedback or comments will be made publicly available and published on the Department of the Attorney-General and Justice website. The Department of the Attorney-General and Justice may draw upon the contents of such and quote from them or refer to them in reports, which may be made publicly available.

Any requests made to the Department of the Attorney-General and Justice for access to a confidential submission, feedback or comment will be determined in accordance with the *Information Act* (NT).

Note: Although every care has been taken in the preparation of the draft review to ensure accuracy, it has been produced for the general guidance only of persons wishing to provide comments on the issues. The contents of the paper do not constitute legal advice or legal information and they do not constitute Government policy documents.

3 Policy Goals

In developing this 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 IPPs.** The OIC'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.

- **not unduly onerous.** The application of the exemption should not require some extraordinary amount of paperwork or the presentation of expert evidence.

4 Applicable Emergency Factual Scenarios

There are three kinds of emergency factual scenarios:

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

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

- 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 NT.

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 year 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.

5 The Information privacy Principles

The Information Privacy Principles (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.

5.1 Current Provisions of the Information Act that dis-apply the information Privacy Principles

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

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. The section reads:

A law enforcement agency is not required to comply with an IPP if the agency believes on reasonable grounds that non-compliance is necessary for one or more of its or another law enforcement agency's functions, including the following:

a) to prevent, detect, investigate, prosecute or punish the commission of an offence against a law of the Territory or any other offence or breach of a law imposing a penalty or sanction for a breach;
b) to manage property seized or restrained under laws relating to the confiscation of the proceeds of crime or the enforcement of those laws or orders under those laws;
c) to execute or implement an order or decision of a court or tribunal, including to execute warrants, to provide correctional services and to make decisions relating to the release of a person from lawful custody;
d) to locate missing persons and next of kin;
e) to provide services in emergency and disaster situations;
f) if the agency is the Police Force of the Northern Territory – its community policing function.

A 'law enforcement agency' is defined in section 4 of the Information Act as follows:

a) law enforcement agency means:
b) the Police Force of the Northern Territory; or
c) the police force of the Commonwealth or of a State or another Territory of the Commonwealth; or
d) the Australian Crime Commission; or
e) 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:
    (iv) preventing, detecting, investigating, prosecuting or punishing the commission of offences;
    (v) 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;
    (vi) protecting public revenue;
    (vii) executing or implementing a decision, direction, order or other requirement of a court or tribunal, including executing warrants.

Section 70(d) of the Information Act clearly gives the Northern Territory Police Force broad powers to use the information it holds for the purpose of locating missing persons and next of kin.

Section 70(e) refers to providing services in emergency and disaster situations.

As a consequence of the definition of "law enforcement agency", it is unlikely that these powers extend to the Northern Territory Emergency Service. It is also unclear whether a declaration of a state of disaster under section 35(3) of the Disasters Act or a declaration of a state of emergency under section 39(2) of the Disasters Act must exist before it is permissible for a law enforcement agency to dispense or fail to comply with the requirements under the IPPs.

Although the Northern Territory Police Service holds a large amount of information about people, it may be essential to gain access to the personal information that is held by other public sector organisations to provide services in emergency and disaster situations.

Option 1: Section 70 be amended so that it applies to NT Emergency Services as well as to law enforcement agencies.

Secondary purposes – emergency situations

In an emergency situation, many people would reasonably expect a public sector organisation to use or disclose personal information for an extended range of purposes related to relief and rescue purposes. The relevant Northern Territory legislation regarding reasonably expected use of information for a secondary purpose is the IPP 2:

2.1 A public sector organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose for collecting it unless one or more of the following apply:

(a) if the information is sensitive information:
(i) the secondary purpose is directly related to the primary purpose; and
(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
(b) if the information is not sensitive information:
(i) the secondary purpose is related to the primary purpose; and
(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
...

Public sector organisations sometimes state on their information collecting forms that a person's information will only be used for specific purposes. It would be difficult to argue that the disclosure of information in an emergency is related, or directly related, to the primary purpose of collection if people have been informed that their information will only be used for that specific purpose. An example is the assurance of specific use given by Territory Housing as follows:

Territory Housing collects only that personal information which is necessary to provide housing assistance under the Housing Act and its Regulations. If you do not provide the

information we may not be able to provide you with assistance. The information collected will not be disclosed to anyone without your consent unless it is required or authorised by law or necessary for maintenance, debt recovery, housing policy and research purposes in accordance with the Information Privacy Principles scheduled in the Information Act (NT). You have a right to access and correct the information held about you. If you have any queries or concerns please contact the Information Management Unit on 08 8999 8490 or write to GPO Box 4621, Darwin NT 0801.

5.2 Secondary purposes - serious and Imminent threats

IPP 2.1 also permits use or disclosure for a secondary purpose if:

(d) 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;

Under the *Information Privacy Act 2000* (Vic), IPP 2.1(d) uses the same wording as the NT IPP 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.

Under the Northern Territory IPP 2.1(d)(i), it is insufficient for an organisation to form a reasonable belief that there is a serious, and in the case of an individual, an imminent threat. It also requires that the organisation believes that it is necessary to disclose the information, in order to lessen or prevent the threat.

IPP 2.1(d)(i) relates only to a threat posed to an individual which is unlikely to be of assistance in a large scale emergency dealing with lots of people. The language 'imminent threat' also implies that the information can only be used or disclosed prior to the threat materialising. This would not allow for the continued use or disclosure of the information after the specific threat has occurred. For example, information could be used or disclosed prior to the onset of a cyclone but not after a cyclone while clean up and recovery efforts are occurring.

IPP 2.1(d) does not specify who can use the information or to whom it can be disclosed. By their nature, emergency circumstances are not common and the recipient organisation would need to be an organisation that is in a position to lessen or prevent the particular threat, such as the Police, or the Department of Health, or the Northern Territory Emergency Service.

The disadvantage of amending the provision so that it includes "public welfare" is that this amendment fails to offer the certainty needed to address the issue. 'Public welfare' is a term open to a wide degree of interpretation. If interpreted narrowly this option may fail to permit the information sharing needed in an emergency, and if interpreted broadly could permit unintended information sharing. For example, an organisation might argue that the names and addresses of persons with criminal records could be released on the basis that this would address a 'serious threat to public welfare'.

The operation of the Victorian exemption 'may' cover post-disaster relief efforts—the question has never actually been tested.

The second concern is that this test offers no mechanism to restore adherence to the IPPs when emergency information sharing is no longer necessary.

Option 2: The 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.

The Information Commissioner has indicated that she does not support this option.

Use or disclosure of information required by law

IPP 2.1(f) permits disclosures that are authorised by law within the Northern Territory.

The problem created by this generic authorisation is that it requires the reader to go to different legislative instruments or the common law to confirm use or disclosure of the information is in fact lawful. A public sector organisation may not have the time or resources to conduct this research in a disaster or emergency. IPP 9 regulates when public sector organisations can transfer personal information about an individual to another person outside of the Northern Territory. IPP 9.1(a) permits disclosures that are authorised under a law of the Territory or the Commonwealth and also suffers from the same problem created by the generic authorisation in IPP 2.1(f).

A provision within the *Information Act* itself that explicitly allows for personal information to be freely exchanged between public sector organisations and other organisations within or outside of the Northern Territory to provide aid, relief, and rescue or recovery assistance during or after a disaster or emergency would remove doubt about the lawfulness of disclosure in a disaster or emergency or the aftermath of a disaster or emergency.

6 New Zealand Code

New Zealand has recently released the Civil Defence National Emergencies (Information Sharing) Code (the New Zealand Code) which permits broad information sharing in the event of national emergencies. It commenced operation 15 April 2013.

The New Zealand Code provides public sector agencies with a broad discretion to collect, use and disclose personal information in the event of a major disaster that triggers a state of national emergency. The Code facilitates the disclosure of personal information to public sector agencies to assist in the government response to a national emergency. The New Zealand Code also allows public sector agencies to disclose information to persons who are responsible for an individual such as parents, spouses or partners regarding the involvement of that individual in the national emergency. For a copy of the New Zealand Code refer Appendix B.

The definition of emergency is defined in the New Zealand Code as:

(a) the result of any happening, whether natural or otherwise, including, without limitation, any explosion, earthquake, eruption, tsunami, land movement, flood, storm, tornado, cyclone, serious fire, leakage or spillage of any dangerous gas or substance, technological failure, infestation, plague, epidemic, failure of or disruption to an emergency service or a lifeline utility, or actual or imminent attack or warlike act; and

(b) causes or may cause loss of life or injury or illness or distress or in any way endangers the safety of the public or property in New Zealand or any part of New Zealand; and

(c) cannot be dealt with by emergency services, or otherwise requires a significant and co-ordinated response under the Civil Defence Emergency Management Act 2002 (NZ).

The operation of the New Zealand Code is not dependent on any external declaration relating to a state of disaster or emergency pursuant to a legislative instrument. However its scope is limited to emergencies or disasters/emergencies occurring in New Zealand or causing loss of life, injury, and distress or endangering the safety of the public or property in New Zealand.

The words 'in New Zealand or any part of New Zealand' would prevent New Zealand public sector agencies from disclosing, under the Code, personal information about New Zealand citizens to foreign organisations or governments in the event of an emergency or disaster outside of New Zealand that affects New Zealand citizens.

7 Northern Territory Definition of Emergency

It may be beneficial for any proposed equivalent Northern Territory provision to define a disaster or emergency in a broad, generic manner, similar to the New Zealand Code, to ensure that the operation of the proposed clause is not dependent on an external approval or official declaration. It may also be beneficial to draft a clause with a wider scope than the New Zealand clause so it is capable of capturing emergencies or disasters outside of Australia that may affect Australian citizens. An example of such an event may be the Sari Club bombing in Bali in 2002.

The advantage of this option is that it offers a high degree of certainty. Currently, the *Disasters Act* deals only with states of emergency, however it is understood that a proposal is under consideration to extend the legislation to deal also with localised emergencies with a category of 'Emergency Situations' –a term designed to include the recovery period. It would therefore be a mechanism that could deal with all but international emergencies. A clear start point is a necessary precursor to having a clear end point which triggers action to restore adherence to the IPPs.

Under the proposed amendment, an 'Emergency Situation' would be declared by the Minister and would provide the relevant agencies with the authority to activate the NT All Hazard Emergency Management Arrangements and instigate the activation of agency plans etc. It is intended that an Emergency Situation is not time limited and it can stay in force until cancelled by the Minister upon the completion of a recovery phase.

Assuming the amendments to the *Disasters Act* will proceed, the *Information Act* could be amended to allow greater indulgences in information gathering and sharing that are reasonably required during an Emergency Situation, State of Emergency or State of Disaster. An Emergency Situation could well follow on from a State of Emergency or State of Disaster to enable reasonable information sharing during the recovery phase. If an Emergency Situation did not follow, or 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 Information Commissioner prefers an exemption linked to the *Disasters Act* rather than a separate test under the *Information Act*. A linked exemption is clearly justifiable and has the advantage of simplicity, rather than a need to apply multiple legislative tests.

Any such exemption would only allow information sharing for limited 'permitted purposes' such as those set out in the New Zealand legislation discussed in this issues paper.

Option 3: That the *Information Act* be amended to insert a provision that provides:

1. 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);

2. 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

3. '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.

An amendment in line with option 3 would eliminate uncertainty surrounding the lawful exchange of personal information from public sector organisations in an emergency or disaster within and outside of the NT. However a number of issues may arise with the implementation of such a broad power. If an 'emergency or disaster' is defined broadly instead of being linked to an external declaration based in the *Disasters Act*, it will become a matter of individual discretion as to whether a situation would constitute a disaster or emergency. This uncertainty can be ameliorated by making the definition of emergency of disaster as descriptive as possible, similar to the definition of emergency in the New Zealand Code.

The New Zealand Code states in clause 3(2), that the Code 'continues to apply... for a further 20 working days after the date on which a state of national emergency expires or is terminated'. A state of national emergency is declared by the Minister under section 66 of the *Civil Defence Emergency Management Act 2002*, when an emergency has occurred or may occur; and the emergency is or is likely to be, of such extent, magnitude, or severity that the management necessary is likely to be beyond the resources of the Civil Defence Emergency Management Groups. Section 3 provides a clear and unambiguous time frame for the operation of the New Zealand Code.

If the *Information Act* is amended so as to permit the continued use, collection or disclosure of information for a period following an event that constitutes an emergency or disaster and the definition of emergency or disaster is not linked to any external declaration, there may be doubt about when an emergency commences or ceases and accordingly how long the proposed provision operates. This may become problematic, for example, in circumstances where a cyclone is downgraded to a tropical storm and subsequently upgraded back to a cyclone.

The declaration of a state of disaster or state of emergency in the *Disasters Act* is limited to events occurring in and/or affecting a part of the Northern Territory. Therefore if the proposed amendment is to be used to assist in disasters or emergencies that occur outside of the Northern Territory, the operation of the provision cannot be linked to declarations under the *Disasters Act*.

8 Sensitive Information

A concern that may arise as a result of the introduction of a broad, discretion based power is the potential for abuse of sensitive personal information. The *Information Act* defines 'sensitive information' to include matters such as sexual preferences or practices, criminal record and health information. IPP 2 Use and Disclosure establishes different procedures for dealing with sensitive and non-sensitive information. Option 3 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 personal information.

There is a strong argument that even in an emergency or disaster situation, public sector organisations should treat sensitive information with a higher level of scrutiny than non-sensitive information. Option 3 may facilitate the disclosure of sensitive personal information to other organisations that do not have satisfactory protections or procedures for the safe keeping of the disclosed information. This could result in privacy breaches as a consequence of the disclosure.

The New Zealand Code 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 co-ordination and management of an emergency. Clause 5 of the New Zealand Code reads:

9 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.

Note: *This clause is based upon Privacy Act 1988 (Australia), Part VIA, in particular, s.80H.*

It may not be practical to distinguish between sensitive and non-sensitive information in the proposed NT amendment, primarily because this may create unrealistic demands on public sector organisations, such as requiring time consuming editing or redacting of large information databases. The risk of abuse or inadvertent privacy invasions may be reduced by adopting a more prescriptive approach to creating boundaries for the use, collection or disclosure of information, such as the use of 'permitted purposes' in the New Zealand Code.

10 Emergencies – End Points

There are several options for an endpoint to an emergency information-sharing exemption:

- a organisation-monitored end-point, where organisations are trusted to assess and determine when information sharing is no longer necessary under the exemption;

- a structured organisation-monitored end-point, where organisations are required to assess and determine when information sharing is no longer necessary under the exemption, in accordance with a time frame;

- an Information Commissioner monitored end-point, where organisations must notify the Commissioner within, say, 28 days of using the exemption and require Commissioner approval to extend use of the exemption for a further 28 days;

- a hybrid approach, where the organisation *may* choose to self-monitor or choose to seek clarity from the Commissioner, and any approval from the Commissioner is of assistance in the event of a privacy complaint made against the organisation.

- a legislative approach where the period of exemption is defined by specific time limits.

- 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.*

The Information Commissioner is of the view that having a definition of a disaster in the *Information Act* in addition to the *Disasters Act* may create additional confusion. However, if any such exemption was created, it could focus on the disruption to information systems by a disaster rather than just the existence of a disaster per se.

One great feature of the New Zealand model is the prescriptive definition of permitted purposes, and the Information Commissioner would like to see this incorporated into whatever amendment is finally adopted.

If a definition of disaster is included in the *Information Act,* the Information Commissioner believes it would need to include some kind of clear time period, similarly to the NZ legislation, in order to ensure that a return to the IPPs is implemented when the time period is over.

In respect of the various options listed above concerning end points, it seems doubtful that that the majority of public sector organisations could appropriately "self-monitor:. A second consideration is how the mechanism would work when multiple agencies are involved. For example, suppose that following a flood in a community, the health clinic seeks to share information with the school, exemptions would be required for both the Department of Health and the Department of Education and Children's Services. This could rapidly become confusing or lead to inconsistencies if responsibility rested at an organisational level.

The preferred option for events within the Northern Territory is the final option above which defines the period of greater information sharing but retains more flexibility than a defined legislative time limit.

Option 4: that 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.*

11 Process for the making of Codes of Practice in the Northern Territory

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. 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.

The Information Commissioner has noted that the current mechanisms for developing a Code of Practice are onerous and could be simplified. Currently, a Code must be recommended by the Commissioner, then put forward by the Minister on behalf of the Department seeking the Code, then approved by the Administrator and Gazetted. 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. It is difficult to see what these extra steps accomplish except for a lot of red tape. If it is considered that 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.

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.

The NT Information Commissioner, Ms Brenda Monaghan has advised that she does not support option 6. Ms Monaghan suggests that a measure that allows Ministers to independently issue a Code of Practice for their own Department without consultation and approval by the Commissioner would not be supported as the Commissioner acts as a safeguard of both privacy and transparency.

Option 5: Codes of practice should be made by either the Minister or the Information Commissioner and that grants of authorization cover all IPPs.

12 Interstate or Overseas Emergencies

In the case of the Thailand tsunami, biometric data was shared between a 33 country task-force jointly shared data to identify the bodies. It is not clear what security measures were taken with the information, or what happened with it when the task force no longer needed it. If the proposed amendment is to override IPP 9 in an emergency and post-emergency situation, the following qualifications should be considered:

- Individuals can have the option to add their names to a register which prohibits transferring their biometric data outside the jurisdiction if this be prohibited but for the new 'emergency exemption'. It is the individual who bears the risk of identity theft, and who should be able to make the choice as to whether the possible identification of their deceased body in the event of a disaster justifies that risk.

- Even in an emergency, biometric data should only be shared with organisations in jurisdictions that do not have similar privacy regimes when justified by the public interest.

- Biometric and other sensitive data should only be shared if it will be stored securely, and if the receiving body agrees to destroy the data after it is no longer being used for the purposes permitted by the 'emergency exemption'.

The approval and gazettal of a Code of Practice under Part 5 Division 3 of the *Information Act* is also an alternative in the event of a disaster overseas affecting the personal information of Territorians.

13 APPENDIX A

Schedule 2 Information Privacy Principles

section 65(1)

13.1 IPP 1 Collection

1.1 A public sector organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 A public sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) a public sector organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that the individual is able to have access to the information; and

(c) the purpose for which the information is collected; and

(d) the persons or bodies, or classes of persons or bodies, to which the organisation usually discloses information of the same kind; and

(e) any law that requires the particular information to be collected; and

(f) any consequences for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, a public sector organisation must collect personal information about an individual only from the individual.

1.5 If a public sector organisation collects personal information about an individual from another person, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of the individual or another individual.

13.2 IPP 2 Use and disclosure

1.1 A public sector organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose for collecting it unless one or more of the following apply:

(a) if the information is sensitive information:

(i) the secondary purpose is directly related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(b) if the information is not sensitive information:

(i) the secondary purpose is related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

(c) the individual consents to the use or disclosure of the information;

(ca) the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest and the following apply:

(i) the research, compilation or analysis will not be published in a form that identifies the individual;

(ii) it is impracticable for the organisation to seek the individual's consent before the use or disclosure;

(iii) in the case of disclosure – the organisation reasonably believes the recipient of the information will not disclose the information;

(iv) if the information is health information – the use or disclosure is in accordance with guidelines issued by the Commissioner under section 86(1)(a)(iv) for this paragraph;

(d) 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;

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(f) the use or disclosure is required or authorised by law;

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;

(ii) enforcing a law relating to the confiscation of proceeds of crime;

(iii) protecting public revenue;

(iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;

(v) preparing for or conducting proceedings before a court or tribunal or implementing the orders of a court or tribunal;

(h) the Australian Security Intelligence Organisation (ASIO) has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIO authorised by the Director-General of ASIO to receive the information and an officer or employee of ASIO authorised by the Director-General of ASIO to do so has certified in writing that the information is required in connection with the performance of the functions of ASIO;

(i) the Australian Secret Intelligence Service (ASIS) has requested the organisation to disclose the information, the disclosure is made to an officer or employee of ASIS authorised by the Director-General of ASIS to receive the information and an officer or employee of ASIS authorised by the Director-General of ASIS to do so has certified in writing that the information is required in connection with the performance of the functions of ASIS.

Note 1: It is not intended to deter public sector organisations from lawfully co operating with law enforcement agencies in the performance of their functions.

Note 2: IPP 2.1 does not override any existing legal obligations not to disclose personal information. IPP 2.1 does not require a public sector organisation to disclose personal information – a public sector organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: A public sector organisation is also liable to the requirements of IPP 9 if it transfers personal information to a person outside the Territory.

2.2 If a public sector organisation uses or discloses personal information under IPP 2.1(g), the organisation must make a written note of the use or disclosure.

2.3 In this IPP:

child, see section 13 of the Care and Protection of Children Act.

exploitation, see section 16 of the Care and Protection of Children Act.

harm, see section 15 of the Care and Protection of Children Act.

13.3 IPP 3 Data quality

3.1 A public sector organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

13.4 IPP 4 Data security

4.1 A public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 A public sector organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

13.5 IPP 5 Openness

5.1 A public sector organisation must make available to the public a document in which it clearly expresses its policies for the management of personal information that it holds.

5.2 On the request of an individual, a public sector organisation must take reasonable steps to inform the individual of the kind of personal information it holds, why it holds the information and how it collects, holds, uses and discloses the information.

13.6 IPP 6 Access and correction

6.1 If an individual requests a public sector organisation holding personal information about the individual for access to the personal information, the organisation must provide the individual with access to the information except to the extent that:

(a) providing access would pose a serious threat to the life or health of the individual or another individual; or

(b) providing access would prejudice measures for the protection of the health or safety of the public; or

(c) providing access would unreasonably interfere with the privacy of another individual; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way that would prejudice the negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:

(i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;

(ii) enforcing a law relating to the confiscation of proceeds of crime;

(iii) protecting public revenue;

(iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;

(v) preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or

(k) providing access would prejudice:

(i) the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or

(ii) the maintenance of law and order in the Territory.

6.2 However, where providing access under IPP 6.1 would reveal evaluative information generated within a public sector organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

6.3 If a public sector organisation holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date,

the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.4 If:

(a) an individual and a public sector organisation disagree about whether personal information about the individual held by the organisation is accurate, complete or up to date; and

(b) the individual requests the organisation to associate with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date;

the organisation must take reasonable steps to comply with that request.

6.5 A public sector organisation must provide reasons for refusing to provide access to or correct personal information.

6.6 If a public sector organisation charges a fee for providing access to personal information, the fee is not to be excessive.

6.7 If an individual requests a public sector organisation for access to or to correct personal information held by the organisation, the organisation must:

(a) provide access or reasons for refusing access; or

(b) make the correction or provide reasons for refusing to make it; or

(c) provide reasons for the delay in responding to the request;

within a reasonable time.

13.7 IPP 7 Identifiers

7.1 A public sector organisation must not assign unique identifiers to individuals unless it is necessary to enable the organisation to perform its functions efficiently.

7.2 A public sector organisation must not adopt a unique identifier of an individual that has been assigned by another public sector organisation unless:

(a) it is necessary to enable the organisation to perform its functions efficiently; or

(b) it has obtained the consent of the individual to do so; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contract service provider in the performance of its obligations to the outsourcing organisation under a service contract.

7.3 A public sector organisation must not use or disclose a unique identifier assigned to an individual by another public sector organisation unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to that other organisation; or

(b) IPP 2.1(d), (e), (f) or (g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 A public sector organisation must not require an individual to provide a unique identifier in order to obtain a service unless its provision:

(a) is required or authorised by law; or

(b) is in connection with the purpose for which the unique identifier was assigned or for a directly related purpose.

13.8 IPP 8 Anonymity

8.1 A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.

13.9 IPP 9 Transborder data flows

9.1 A public sector organisation must not transfer personal information about an individual to a person (other than the individual) outside the Territory unless:

(a) the transfer is required or authorised under a law of the Territory or the Commonwealth; or

(b) the organisation reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to these IPPs; or

(c) the individual consents to the transfer; or

(d) the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request; or

(e) the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or

(f) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to the transfer;

(iii) it is likely that the individual would consent to the transfer; or

(g) the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred in a manner that is inconsistent with these IPPs.

13.10 IPP 10 Sensitive information

10.1 A public sector organisation must not collect sensitive information about an individual unless:

(a) the individual consents to the collection; or

(b) the organisation is authorised or required by law to collect the information; or

(c) the individual is:

(i) physically or legally incapable of giving consent to the collection; or

(ii) physically unable to communicate his or her consent to the collection;

and collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or

(d) collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

10.2 Despite IPP 10.1, a public sector organisation may collect sensitive information about an individual if:

(a) the collection:

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no other reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

14 APPENDIX B

Civil Defence National Emergencies (Information Sharing) Code 2013

Including notes and Amendment No 1 (Temporary)

This edition of the code includes notes which are set out in italics. This material is not part of the code but is included to assist users of the code.

Privacy Commissioner
Te Mana Matapono Matatapu

Civil Defence National Emergencies (Information Sharing) Code 2013

I, MARIE SHROFF, Privacy Commissioner, having given notice under section 48(1) of the Privacy Act 1993 of my intention to issue a code of practice and having satisfied the other requirements of the subsection, now issue under section 46 of the Act the Civil Defence National Emergencies (Information Sharing) Code 2013.

Issued by me at Wellington on 4 March 2013

The SEAL of the Privacy Commissioner was affixed to this Code of Practice by the Privacy Commissioner) *[L.S.]*

Marie Shroff
Privacy Commissioner

Note: *This code is deemed to be a regulation for the purposes of the Regulations (Disallowance) Act 1989 – Privacy Act, s.50.*

1.

This code of practice may be referred to as the Civil Defence National Emergencies (Information Sharing) Code 2013.

2. Commencement

This code will come into force on 15 April 2013.

Note: *Amendment No 1 (Temporary) also commenced 15 April 2013 (and expires 14 April 2014).*

3. Application to a state of national emergency

(1) To assist with the effective management of the response to a national emergency, this code applies in relation to any emergency in respect of which a state of national emergency is in force.

(2) To assist with the recovery from a national emergency, this code continues to apply in relation to such an emergency for a further 20 working days after the date on which a state of national emergency expires or is terminated.

4. Interpretation

In this code:

emergency has the same meaning as in section 4 of the Civil Defence Emergency Management Act 2002

state of national emergency means a state of national emergency declared under section 66 of the Civil Defence Emergency Management Act 2002

permitted purpose has the meaning set out in [clause 5].

***Note**: The Civil Defence Emergency Management Act defines **emergency** to mean a situation that:*

(a) is the result of any happening, whether natural or otherwise, including, without limitation, any explosion, earthquake, eruption, tsunami, land movement, flood, storm, tornado, cyclone, serious fire, leakage or spillage of any dangerous gas or substance, technological failure, infestation, plague, epidemic, failure of or disruption to an emergency service or a lifeline utility, or actual or imminent attack or warlike act; and

(b) causes or may cause loss of life or injury or illness or distress or in any way endangers the safety of the public or property in New Zealand or any part of New Zealand; and

(c) cannot be dealt with by emergency services, or otherwise requires a significant and co-ordinated response under the 2002 Act.

***Note**: Amendment No 1 corrected an error in the definition of permitted purpose and substituted reference to clause 5 for the incorrect reference to clause 4.*

***Note:** Several terms used in the code are defined in the Privacy Act including e.g. agency, collect, enactment, individual, information privacy principle, news medium, personal information, public sector agency – Privacy Act, s.2.*

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 sub clause (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.

Note: *This clause is based upon Privacy Act 1988 (Australia), Part VIA, in particular, s.80H.*

6. Authority for collection, use and disclosure of personal information

(1) In relation to an emergency, an agency may collect, use or disclose personal information relating to an individual if the agency believes on reasonable grounds that:

(a) the individual concerned may be involved in the emergency; and

(b) the collection, use or disclosure is for a permitted purpose in relation to the emergency; and

(c) in the case of a disclosure of personal information - the disclosure is to:

(i) a public sector agency; or

(ii) an agency that is, or is likely to be, involved in managing, or assisting in the management of, the emergency; or

(iii) an agency that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency; or

(iv) a person who is **responsible** for the individual (within the meaning of [clause 5(3))]; and

Note: Amendment No 1 corrected an error in paragraph (iv) and substituted reference to clause 5(3) for the incorrect reference to clause 4(3).

(d) in the case of a disclosure of personal information – the disclosure is not to a news medium.

Note: *This subclause is based upon Privacy Act 1988 (Australia), Part VIA, in particular, s.80P.*

Note: *Questions of disclosure of personal information to a news media organisation are not affected by this code and are subject to any normal legal considerations under the Privacy Act or applicable law such as the Official Information Act 1982. This code applies no additional restrictions to such disclosures nor does it relax normal constraints.*

(2) The authority in subclause (1) is in addition to, and does not restrict, any other authority for collection, use or disclosure contained in the information privacy principles, any code of practice or other enactment.

(3) The authority in subclause (1) is not limited to collection, use and disclosure of personal information by agencies within the district directly affected by the emergency.

Explanatory note

This code modifies the application of the applicable information privacy principles by providing that, where the code applies, agencies are authorised in certain circumstances to collect, use or disclose personal information for certain permitted purposes related to the government response to a national emergency.

The code comes into effect in relation to any emergency for which a state of national emergency is in effect. The code continues in effect after the expiry of a state of emergency for a further 20 working days in relation to the emergency.

Civil Defence National Emergencies (Information Sharing) Code 2013
Amendment No 1 (Temporary)

I, MARIE SHROFF, Privacy Commissioner, now issue under section 51 of the Privacy Act 1993 the Civil Defence National Emergencies (Information Sharing) Code 2013 Amendment No 1 (Temporary).

Issued by me at Wellington on 5 March 2013
The SEAL of the Privacy Commissioner was)
affixed to this Amendment to the Civil Defence)
National Emergencies (Information Sharing))
Code 2013 by the Privacy Commissioner)

Marie Shroff

Privacy Commissioner

1. Title

This amendment is the Civil Defence National Emergencies (Information Sharing) Code 2013 Amendment No 1 (Temporary).

2. Commencement

This amendment will:
(a) come into force on 15 April 2013; and
(b) expire on 14 April 2014.

3. Amendment to clauses 4 and 6(1)

Clause 4 and clause 6(1) are amended in the following manner:

Reference	Delete	Replace with
Clause 4 (within the definition of **permitted purpose**)	clause 4	clause 5
Clause 6(1)(c)(iv)	clause 4(3)	clause 5(3)

Note: *This amendment corrects numbering errors in two cross-references.*

Legislative history

12 April 2012 – Public notice of intention to issue code.
4 March 2013 - Code issued
5 March 2013 – Amendment No 1 (Temporary) issued.
7 March 2013 – Notice in New Zealand Gazette