

Large scale emergencies and personal information
– can the Privacy Act cope?

Katherine Gibson

I Introduction

In times of large scale disasters are the current data protection provisions in the Privacy Act appropriate, or could they inhibit the rescue and relief mission undertaken to handle the emergency. No one would dispute the appropriateness of sharing necessary personal information to assist in handling rare, large scale emergencies - the issue is getting the right balance between achieving this objective and ensuring there are enough safeguards in place to protect the privacy of the individual in these unusual circumstances. As aptly put by one Australian Senator:¹

We would all like to assist where we can in these times of emergency and appreciate the need for individuals and aid agencies to access necessary information. In these traumatic situations, Australians expect information to be accessible in order to assist in the disasters. They expect no less information than necessary but also no more than needed would be made available.

Recently, in response to the destructive earthquake that struck Christchurch on 22 February 2011, the Privacy Commissioner issued a code permitting agencies to collect, use and disclose personal information of victims of the earthquake for the purpose of assisting in dealing with the emergency. This paper will consider whether the current legislation in New Zealand is flexible enough to allow necessary and appropriate handling of personal information when a large scale emergency such as the earthquake occurs, whether the code was required and some options for reform.²

¹ (17 October 2006) 12 CthAPD 6.

² This paper will only consider whether the law permits such actions, and not requires. If the law permits such actions, it is still at the discretion of the agency as to whether they take such steps. They may have other considerations or overriding obligations which mean they decide not to do so.

II Christchurch Earthquake Code

A Background

For some time, the Privacy Commissioner's Office has been keeping an eye on the performance of data protection laws overseas where large scale disasters have occurred, such as the Bali bombings in 2002, Hurricane Katrina in 2005 and the 2004 Boxing Day tsunamis. Of particular interest, given the similarities in the data protection legislation between the two countries, was the amendment to the Australian Privacy Act in 2006,³ which was in the main in response to the experiences encountered by those involved in the emergency relief in the handling of personal information after the Boxing Day tsunamis. This amendment inserted a new Part VIA into the Act to make special provision for the collection, use and disclosure of personal information when an emergency or disaster occurs.⁴

In a report to the Minister of Justice on the review of the operation of the New Zealand Privacy Act in May 2008, the Privacy Commissioner referred to the reports of difficulties encountered in Australia and Canada with the data protection laws and that those laws may have inhibited the disaster relief and identification of victims and survivors of the Boxing Day tsunamis.⁵ The Commissioner noted that she was not aware of any significant problem with the New Zealand Act, or whether any particular amendment needed to be made, however, given the amendment to the Australian Act, the Commissioner recommended that disaster management officials give consideration to whether any amendment is “*desirable to provide for best practice disaster information management in the event of a declared emergency and, in particular, whether any amendments such as those adopted in Australia are useful*”.⁶ To date, the Law Commission has not made a recommendation on this issue.

So well before the earthquake struck in 2011, the Commissioner's office was alive to the potential difficulties that may be encountered by organisations needing to share personal

³ Privacy Legislation Amendment (Emergencies and Disasters) Act 2006 (Australia).

⁴ Privacy Act 1988 (Australia), s80F.

⁵ Privacy Commissioner *Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) - Fourth supplement to the first periodic review of the operation of the Privacy Act 1993*” (2008).

⁶ *Ibid* at [2.17].

information after a large scale disaster so that they could effect the rescue, recovery and rehabilitation of the victims.

B Issuing the Earthquake Code

The day after the Christchurch earthquake, a state of national emergency was declared⁷ and it became clear very quickly that this could be one of New Zealand's worst natural disasters.⁸

Around 48 hours after the massive earthquake struck, on 24 February 2011 the Commissioner issued the Christchurch Earthquake Code 2011 ("Code")⁹ to commence at 5pm on that day.¹⁰ The Commissioner issued the Code under the urgency procedure, dispensing with the requirements to notify of an intention to issue a code and undertake consultation on the proposed code with stakeholders.¹¹

Initially the Code was to expire on 24 May 2011 or on the expiry of the declaration of emergency, whichever came first, however, the Code was later amended to expire on the fixed date of 24 May 2011.¹²

The Commissioner in her letter to the Regulations Review Committee advising of the issuing of the Code, made the following comments:¹³

While notification and consultation was not possible on this occasion, I nonetheless was cautious and adopted what I believed to be a proportionate approach that reconciles the important public objectives of facilitating emergency response while safeguarding privacy. In particular, I modeled my code closely upon legislation adopted in an amendment to the Australian Privacy Act 1988 (see Part VIA).

Commenting on the need for the Code, the Commissioner said:¹⁴

⁷ This was declared under the Civil Defence Emergency Management Act 2002 and was extended a number of times until 30 April 2011. Under the Act, a state of emergency can only be declared for a maximum of seven days at one time.

⁸ Whilst some bodies are yet to be identified, Police believe the death toll will be 182. "Christchurch earthquake death toll reaches 182" 17 March 2011 <www.stuff.co.nz>.

⁹ Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

¹⁰ The Commissioner has the power to issue a code of practice, which can modify the application of the Information Privacy Principles, Privacy Act 1983, s46.

¹¹ Privacy Act 1983, ss47, 48.

¹² Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) Amendment No.1.

¹³ Letter from Privacy Commissioner to Regulations Review Committee regarding the Code (2 March 2011) at 1.

¹⁴ *Ibid*, at 2.

The code was a precaution to provide agencies involved in responding to the emergency, and other agencies interacting with them and with victims' families, reassurance by providing supplementary authority to share information as needed. I was not reacting to specific problems that had been encountered but instead trying to act pre-emptively to diminish the likelihood of barriers to disclosure in the emergency.

Additionally, in a media release on the Code, the Office of the Privacy Commissioner said “*Although the Privacy Act already allows disclosure of information for public safety, law enforcement and health reasons, the code provides greater certainty and broader discretion at this critical time*”.¹⁵

The Commissioner had not formed the view that the Code was necessary but drawing from overseas experiences felt it was appropriate so that difficulties were not encountered in the emergency effort due to concerns about whether the Privacy Act allowed certain personal information practices.¹⁶

C Australia

The Code was based on an amendment made to the Australian Federal Privacy legislation in 2006. Given the similarities in the relevant legislation, the Australian experience is instructive for New Zealand in these circumstances.¹⁷

The data privacy issues faced by Australia in large scale disasters were considered in 2005. The Federal Privacy Commissioner noted the issue as follows:¹⁸

¹⁵ “Extension of Christchurch Earthquake (Information Sharing) Code” (media release, 11 March 2011).

¹⁶ The Code highlights the powers of the Commissioner being able to issue an urgent code under the Act in these circumstances without any further legislation being enacted. Compare this to the Canterbury Earthquake Response and Recovery Act 2010 which was hurriedly enacted after the first Christchurch earthquake in 2010 to facilitate the response to the Canterbury earthquake and to enable, amongst other things, by an Order in Council, the relaxation or suspension of provisions in enactments that may not be reasonably capable of being complied with owing to circumstances resulting from the Canterbury earthquake (including any of its aftershocks).

¹⁷ Unlike New Zealand, the Australian Federal Privacy Commissioner does not have the power to issue an urgent code. There is the power to make an urgent temporary public interest determination (“TPID”) where the public interest in the act that breaches the Act outweighs to a substantial degree the public interest in adhering to the Act. The effect of a TPID is that the act is not a contravention of the Act. A TPID can only be issued on an application by an agency or organisation, and is not appropriate in large scale emergency situations, where quick action is vital. Privacy Act 1988 (Australia) ss 80A, 80B.

¹⁸ Australian Government – Office of the Privacy Commissioner *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*(2005) at 235.

The scale and gravity of large scale emergencies have tested the application of the Privacy Act and raised questions as to how privacy protection should operate in such situations. The Privacy Act received criticism in the media after the tsunami disaster for lacking commonsense and for being unable to anticipate and cope with the extent of the tsunami disaster.

In particular, considering National Privacy Principle 2 (“NPP2”),¹⁹ the Commissioner acknowledged that disclosure by the airlines to families and friends of information about whether missing people had caught planes after the tsunami hit “*would normally appear to be a breach of NPP2*”.²⁰ Of particular relevance to New Zealand is that NPP2 includes a health and safety exception similar to the New Zealand Act.²¹ The Commissioner must have formed the view that the health and safety exception does not apply in these circumstances.

Later in 2005, the Legal and Constitutional References Committee reported that the Act was found to be an impediment to information sharing between government and non-government agencies in the response and recovery in emergency situations that occurred overseas.²²

In response to the issues raised, an amendment bill was introduced in 2006 proposing to inserting a new Part VIA into the Act.²³ The submissions received by the Committee charged with inquiring into the Bill²⁴ broadly supported an amendment to the Privacy Act to provide clarity in this area and to allow the appropriate responses to an emergency or disaster. There were differences of opinion in how this outcome should be achieved.²⁵ The question of whether the current legislation was flexible enough in its current form to allow the required collection, uses and disclosures was not considered in any detail in the reports on the Bill, other than repeating the equivocal quote by the Commissioner in relation to the NPP2 discussed above.

¹⁹ Privacy Act 1988 (Australia), Sch3. Generally, NPP2 does not permit disclosure of personal information for a purpose other than the primary purpose of collection except with the consent of the individual, or in circumstances where one of the other exceptions in NPP2 applies.

²⁰ *Report on Privacy Act*, at 234, above n 18.

²¹ Discussed at pages 12-14.

²² The Senate - Legal and Constitutional References Committee *The real Big Brother: Inquiry into the Privacy Act 1988* (2005).

²³ Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Australia).

²⁴ Senate Standing Committee on Legal and Constitutional Affairs.

²⁵ 13 submissions were received by the Committee and the enquiry was dealt with on the papers. The number of submissions may be due to short time given to submitters– submissions were called for on about 14 September 2006, to be provided by 25 September 2006.

Some expressed views that the Act did not need amending and was “adequate to facilitate the information flows contemplated by the amendments”²⁶ and “already permits virtually all reasonable responses to emergencies envisaged by this proposed amendment”.²⁷

The explanatory memorandum on the Bill provided no clear statement on whether the Act permitted the required information practices necessary in these exceptional situations, rather.²⁸

The Privacy Act already has exemptions concerning use and disclosure of personal information that afford agencies and organisations some flexibility in an emergency or disaster situation. However, these have proven difficult to apply with confidence in crises involving mass casualties and missing persons, because of uncertainty as to the extent of their application. Part VIA of the Bill is aimed at addressing the practical issues faced by agencies, the private sector and non-government organisations, which were highlighted during events such as the Asian tsunami in December 2004.

Notwithstanding the lack of a detailed review of the provisions of the Act in the reports, it was clear that difficulties were experienced in applying the Act in these unusual times and amendments were required.

²⁶ Office of the Victorian Privacy Commissioner *Inquiry into Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006) at 1.

²⁷ Australian Privacy Foundation *Re Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006) at 1.

²⁸ The Parliament of Australia – House of Representatives *Privacy Legislation Amendment (emergencies and Disasters) Bill 2006, Revised Explanatory Memorandum* (2006) at 1.

D The Code

For the purpose of the analysis that follows in Section IV, the main provisions of the Code are repeated in full.

Subclause 5(1) provides:

- (1) In relation to the Christchurch earthquake 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 4(3)); and
 - (d) in the case of a disclosure of personal information – the disclosure is not to a news medium.

This is based on an Australian provision.²⁹

The permissions in the Code are in addition to, and do not restrict the Information Privacy Principles, any other code of practice issued under the Privacy Act or other enactment.³⁰

An agency is an individual or an organisation (whether incorporated or not) in both the public and private sectors.³¹

²⁹ Privacy Act 1988 (Australia), s80P.

³⁰ Code, cl5(2).

³¹ Privacy Act 1983, s2(1).

Clause 4 provides:

(1) A **permitted purpose** is a purpose that directly relates to the government and local government response to the Christchurch earthquake emergency in respect of which an emergency declaration exists.

(2) Without limiting subclause (1), any of the following is a **permitted purpose** in relation to the Christchurch earthquake 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.

This is based on an Australian provision.³²

³² Privacy Act 1988 (Australia), s80H.

III Current Legislation

A Personal information requirements in a disaster

In times of large scale disasters, personal information, including sensitive health information, will be required urgently to assist in handling the emergency. Some examples arising from the earthquake may be:

- Dental and medical records for identification purposes.
- Details of the travel and accommodation plans of tourists to eliminate those individuals who may have been caught up in the disaster. This information would be held by travel agencies, airlines and hotels.
- Names of workers who were normally “at their desks” at the time of the earthquake in the badly affected buildings. This information would be held by employers and work colleagues.
- Names of students who were scheduled to be in a class in the CTV building at the time of the earthquake. This information would be held by the school.
- Sharing information about deceased, missing and injured people between the agencies assisting in the emergency effort.

B Relevant legislation

The Act contains 12 Information Privacy Principles (“IPPs”) that govern how organisations and individuals collect, use, store and disclose personal information.³³ Generally, the IPPs require an agency:

- must collect personal information directly from the individual, or from another source if authorised by the individual;
- that obtains personal information in connection with one purpose shall not use the information for any other purpose unless the use for the other purpose is authorised by the individual concerned;

³³ Personal information is information about an identifiable individual, being a natural person, not being a deceased person. Privacy Act 1993, s2(1).

- shall not disclose personal information to a third party unless it is one of the purposes in connection with which the information was obtained or the disclosure is authorised by the individual concerned.

In addition to the IPPs, the Health Information Privacy Code 1994 (“HIPC”) and the Health Act 1956 governs the handling of health information. The HIPC applies to all health information³⁴ and all health agencies (large or small, public or private).³⁵ The IPPs are modified by the HIPC to the extent that personal information is health information and an agency is a health agency. The HIPC follows the same structure as the IPPs, with 12 Rules.

Considering the information requirements in a disaster, immediately issues arise:

- individuals are missing or incapacitated and cannot authorise the collection of personal information by those managing the emergency;
- in most circumstances the collection of personal information by agencies before the earthquake struck (for example, people’s travel plans, or information about students attending classes) would not be for a purpose related to assisting in a large scale emergency, and the individuals cannot provide the requisite authorisation for this information to be disclosed for another purpose.

Both agencies in the exchange of the personal information (the collector and the discloser) will have to consider whether any of the exceptions in the IPPs apply to allow the sharing of information for this purpose.³⁶ An important feature of the Act is there will be an action of interference with the privacy of an individual only if there is a breach of an IPP or a code of practice and harm or significant humiliation or loss of dignity has or may be caused to the individual concerned.³⁷ If the individual cannot show harm, there will be no interference with privacy under the Act. Where the intended information practice is not permitted under the Act a practical answer in these unusual circumstances of a large scale emergency may be that it is unlikely that harm or humiliation would result, or that the individual concerned would

³⁴ HIPC, s4(1).

³⁵ HIPC, s4(2).

³⁶ If an agency relies on any exception then the onus of proving the exception is on the agency, Privacy Act 1993 s87.

³⁷ Privacy Act 1993, s66. Note the exceptions to this, which are not relevant in these circumstances ss66(2)-(4).

complain.³⁸ Agencies should not have to rely on this - it is inconsistent with good governance and certainly not a satisfactory answer in the long term.

Generally, collection of personal information in these circumstances will be permitted. Where information is collected for the purpose of assisting in the emergency effort,³⁹ and the individual concerned is missing or otherwise incapacitated, the IPPs⁴⁰ and the HIPC⁴¹ contain exceptions to permit the collection of personal information and health information respectively from a person other than the individual concerned.

It appears the greatest difficulties occur in considering whether the agency holding the personal information is permitted to disclose the information for the purposes of the emergency effort.⁴²

C Disclosure of personal information

1 Personal information

IPP11 provides that an agency that holds personal information shall not disclose the information to a third party unless the agency believes, on reasonable grounds that one of the exceptions listed in IPP11 apply. There are a number of exceptions listed, including where the individual has authorised the disclosure,⁴³ or where the disclosure is “*one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained*”.⁴⁴ Neither exception assists.

³⁸ Note that a complaint can be made by any person and not just the individual concerned, Privacy Act 1983, s67.

³⁹ The information must be collected for a lawful purpose connected with a function or activity of the agency and the collection must be necessary for that purpose, IPP1.

⁴⁰ An agency is permitted to collect information from another source where the agency believes on reasonable grounds that it would not prejudice the interests of the individual concerned (IPP2(2)(c)) or where it is not reasonably practicable in the circumstances to collect the information from the individual concerned (IPP2(2)(f)).

⁴¹ R2(2)(b) permits collection from the individual’s representative or where the representative authorises collection from someone else. In addition, collecting information directly from the individual concerned is not required where the health agency believes on reasonable grounds that it would prejudice the interests of the individual concerned (R2(2)(c)) or it is not reasonably practical in the circumstances of the particular case (R2(2)(d)).

⁴² This paper will not separately consider IPP10 (governing the use of personal information) or R10 HIPC (governing the use of health information). IPP10 and R10 generally raise the same issues as those discussed in relation to the disclosure of personal information and health information.

⁴³ IPP11(d).

⁴⁴ IPP11(a).

IPP11 has a health and safety exception. IPP11(f) permits disclosure where the agency believes, on reasonable grounds:⁴⁵

that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to-

- (i) public health or public safety; or
- (ii) the life or health of the individual concerned or another individual; or

The requirements of this exception are discussed in the mirror exception for health information in the HIPC. This exception will not assist in a large scale disaster that has already occurred and where the individual is missing, dead or cannot be identified.

The Law Commission in its current review of the Privacy Act has proposed that the words “*and imminent*” be deleted from IPP11(f),⁴⁶ however this would not assist in these circumstances.

2 Health Information

Both the HIPC and the Health Act permit disclosures of health information⁴⁷ in certain circumstances.

(a) Representative

Under the HIPC, a health agency may disclose health information if the health agency believes on reasonable grounds that disclosure is to an individual’s representative or is authorised by the individual’s representative where that individual is dead or is unable to exercise their rights under the rules or give their authority.⁴⁸

The term “*representative*” in the HIPC and Health Act means:⁴⁹

- a. where the individual is dead, the individual’s personal representative (being the deceased person’s executor or administrator);⁵⁰

⁴⁵ IPP11(f).

⁴⁶ Law Commission *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4* (NZLC IP17, 2010) at [4.97].

⁴⁷ Health information under the Health Act is narrower than under the HIPC, however, for these purposes it is not a material difference. Health Act 1956, s22B.

⁴⁸ HIPC, R11(1)(a),(b).

⁴⁹ HIPC, s3; Health Act, s22B.

⁵⁰ HIPC Commentary at 8.

- b. where the individual is under the age of 16 years, the individual's parent or guardian;
- c. where the individual is not dead or under the age of 16 years, and the individual is unable to give consent or authority, a person appearing to be lawfully acting on the individual's behalf or in that individual's interests.

This will assist the disclosure of health information in large scale emergencies, however, requires identifying and locating the representative of the relevant individual, which may not be practical in the circumstances.

(b) HIPC- Rule 11

Similar to IPP11, Rule 11 of the HIPC provides that a health agency that holds health information must not disclose the information unless the agency believes on reasonable grounds that one of the exceptions listed applies. Where the health agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual concerned, Rule 11(2) provides further exceptions including:

- where the information is disclosed by a health practitioner to a near relative of the individual concerned in accordance with recognised professional practice and the disclosure is not contrary to the express request of the individual or his or her representative;⁵¹ or
- where the life or health of an individual may be threatened.⁵²

It is unlikely that the disclosure of health information for assisting a large scale emergency fits within the “recognised professional practice” exception. The ‘health’ exception has a high threshold for the disclosing agency to meet. Indeed the commentary to the Rule states the exception “*should not be used lightly*”.⁵³ For this (and the mirror IPP11(f)) exception to apply, the following must be satisfied:⁵⁴

⁵¹ HIPC, r11(2)(b).

⁵² HIPC, R11(2)(d). This is identical to the exception in IPP11(f).

⁵³ HIPC Commentary, at 65.

⁵⁴ A useful summary of the requirements of the exception is set out in *Case Note 5733* [2001] NZPrivCmr 16.

1. The agency has reasonable grounds to believe that there is a serious threat to:
 - a. public health, or
 - b. public safety; or
 - c. the life or health of the individual concerned; or
 - d. the life or health of another individual.
2. The agency has reasonable grounds to believe that the threat is imminent.
3. Disclosure is to be made to an appropriate or responsible body that has powers to prevent or lessen the threat.⁵⁵
4. The agency has reasonable grounds to believe that disclosure is necessary to prevent or lessen the threat.
5. In addition where a health agency discloses health information, the agency has reasonable grounds to believe that it is neither desirable nor practicable to obtain authorisation from the individual⁵⁶ and the agency must only disclose information to the extent necessary to prevent or lessen the threat.⁵⁷

This exception is aimed at preventing an emergency from happening and will not provide all the necessary permissions where the threat to the life or health of an individual has already occurred and the purpose of the disclosure is to assist in the emergency relief effort.

(c) s22C Health Act

This provision permits disclosure by an agency to specified persons for specified purposes and includes disclosure of health information to any member of the Police for the purposes of exercising or performing any of their powers, duties or functions.^{58 59} This may be of assistance in these circumstances - for example permitting release of dental records for identification purposes.

⁵⁵ *Duncan v Medical Practitioners Disciplinary Committee* [1986] 1 NZLR 513 at 518.

⁵⁶ HIPC, R11(2)(d)(ii).

⁵⁷ HIPC, R11(3).

⁵⁸ Health Act 1965, s22C(2)(f).

⁵⁹ For completeness, the Health Act requires (and not merely permits) disclosure of health information to an individual's representative if a request is made under s22F(1) of that Act.

IV Application of Privacy Act and Code

The following table considers some issues that were, or could have been faced by organisations and individuals as a result of the Christchurch earthquakes⁶⁰ and how the Privacy Act and the Code apply.

⁶⁰ Before the massive February 2011 earthquake, an earthquake had struck Christchurch on 4 September 2010.

Examples of earthquake related enquiries received by the Privacy Commissioner's Office⁶¹

Example	Privacy Act ⁶²	Code applies?	Code required?
An individual made an insurance claim for a damaged computer but objected to the insurer's demand to hand over the hard drive	IPP1 – the insurer will need to show that collection of the personal information on the hard drive is for a lawful purpose connected with the insurance claim and is necessary for that purpose. ⁶³	Code does not apply. Collection is not for a “permitted purpose”.	No. IPP1 appropriate
An individual objected to the fact that EQC had disclosed information to his bank.	Identify what personal information has been disclosed. IPP11 – EQC would have to show it believed on reasonable grounds one of the exceptions applied.	Code does not apply. ⁶⁴ Bank not an agency involved in response (cl 5(1)(c)(ii),(iii)). Disclosure is not for a “permitted purpose”.	No. IPP11 appropriate.
An individual sought access to an insurer's engineer's report which was being withheld by the insurer.	Identify what personal information is held in the engineer's report. IPP6 - request for access. s27- 29 – any reasons for refusal apply?	Code does not apply. Code does not contain provisions relating to access to personal information.	No. IPP6, s27-29 appropriate.
A man was concerned that he was repeatedly being stopped by Police and asked for identification because of the way he looked.	IPP1 – the Police will need to show that collection of the personal information is for a lawful purpose connected with a function of the Police and necessary for that purpose. ⁶⁵	Code does not apply. Code permits collection of personal information relating to an individual where that individual may be involved in the emergency (cl5(a)). This is not the case here.	No. IPP1 appropriate.

⁶¹ These examples were helpfully provided by Blair Stewart, Assistant Commissioner (Auckland). The enquiries were received between 10 September 2010 and 8 March 2011.

⁶² The analysis only considers whether the particular act is permitted under the Privacy Act. Other enactments may apply which will not be considered here.

⁶³ IPP4, manner of collection may also be relevant.

⁶⁴ Assuming the bank requested this information from the EQC as part of its usual commercial activities in lending money to the individual.

⁶⁵ IPP4, manner of collection may also be relevant.

Example	Privacy Act	Code applies?	Code required?
A mental health advocate was trying to work from home despite being injured. Her manager tried to arrange for a client to come to her house for a meeting. She refused to have the meeting at her house and her manager demanded a medical certificate.	IPP1 – the employer will need to show that collection of the medical certificate is for a lawful purpose connected with the employment of the worker and is necessary for that purpose. ⁶⁶	Code does not apply.	No. IPP1 appropriate.
The offices of an organisation had been destroyed in the earthquake and guidance was sought in relation to security and storage of personal information.	IPP5.	Code does not apply. Code does not contain provisions in relation to security and storage.	No. IPP5 appropriate.
A medical centre had received a request from the husband of an apparently deceased earthquake victim for medical records to be made available to assist with identification. The clinic did not know if the deceased had left a will.	Disclosure permitted if the husband is appearing to be lawfully acting on the wife’s behalf or in her interests (R11(1)HPIC). ⁶⁷ The centre appears to have formed the view that the wife is ‘dead’ in considering who is the wife’s “representative” for the purposes of disclosure.	On balance, Code applies and disclosure permitted . Potential issues: - can the centre rely on the advice of the husband that the wife may be involved in the emergency? - dental records are normally used for identification - should further enquiry be made by the centre? - no express requirement in Code for centre to disclose only to the extent necessary for the particular purpose ⁶⁸ - medical records may contain information wife does not want husband to know.	Code assists, although its application raises issues.

⁶⁶ IPP4, manner of collection may also be relevant.

⁶⁷ As the individual is not confirmed dead, the husband does not have to be the wife’s executor or administrator.

⁶⁸ As required where disclosure of health information is made under R11(2), HPIC, R11(3).

Examples	Privacy Act	Code applies?	Code required?
An independent practitioner's association asked about its ability to disclose information to assist Maori health providers from other regions that had come into the city to assist. They had been requested to reveal identities of patients who were affiliated with the iwi.	Disclosure not permitted . R11HIPC – no exceptions apply.	Code may apply. ⁶⁹ Potential issues: - does association have reasonable grounds to believe the individuals may be involved in the emergency. - does association have reasonable grounds to believe health providers are an agency involved in response (cl5(1)(c)(ii), (iii)).	Code may assist.
A public body sought advice as to whether lists of information about students could be disclosed to foreign embassies.	Disclosure not permitted . IPP11 – no exceptions apply.	Code does not apply. Disclosure not permitted . Foreign embassies not an agency involved in managing the emergency (cl5(1)(c)(ii)) or an agency “ <i>directly involved</i> ” in providing the services listed in cl5(1)(c)(iii).	No – there may be a view that disclosure would assist with the emergency - raises issues in application.
A charity had received numerous requests from people to organise fundraising on its behalf. It wanted to know about requiring disclosure of criminal convictions by fundraising organisers.	IPP 1 – the charity will need to show that collection of the criminal convictions is for a lawful purpose connected with the fundraising activities of the charity and the collection is necessary for that purpose.	Code does not apply. Code permits collection of personal information relating to an individual where that individual may be involved in the emergency (cl5(a)). This is not the case here.	No. IPP1 appropriate.

⁶⁹ Further information on the role of the Maori health providers required before a view can be formed.

Other possible examples

Example	Privacy Act	Code applies?	Code required?
<p>An airline had received requests from the Police, family members and friends for details of whether certain individuals that cannot be contacted had flown into or out of Christchurch.</p>	<p>Disclosure not permitted. IPP11 – no exceptions apply.⁷⁰</p>	<p>Disclosure permitted Permitted purpose (cl4(2)(a)). Disclosure permitted to a public sector agency, or a family member or friend if they are a person responsible for the individual (cl4(3)). Potential issue: - what evidence is required for the airline to hold a reasonable belief that the family member or friend is a ‘responsible person’</p>	<p>Yes.</p>
<p>A school whose premises had been badly damaged in the earthquake had received requests from the Police and family members for details of students who were scheduled to be at class at the time of the earthquake.</p>	<p>Disclosure not permitted. IPP11 – no exceptions apply</p>	<p>As per example above disclosure permitted.</p>	<p>Yes.</p>

⁷⁰ If the Police request was in relation to investigating an offence, then IPP11(e)(i) would permit disclosure.

In most examples the Privacy Act can adequately deal with the situation, however there was a need for the Code in some areas.

Even in applying the Code to this small number of examples, issues arise:

- should guidance be given to agencies on what evidence is required to hold a reasonable belief that the individual is involved in the emergency at a time when chaos is the norm, buildings and people's homes have been destroyed, communication links are unstable and there is a need to act quickly - is it informal reports from a family member or friend, confirmation from the person requesting the information, information from the media, or something more formal like a Police report (which would not be required but provides a sense of the spectrum).
- what does "*directly involved*" in providing the services mean?⁷¹
- how do agencies satisfy themselves that "*a person is responsible for an individual*" – the list is clear on who is included, however, what evidence (in difficult times) is required to confirm they are the wife, mother, or relative and a member of the individual's household.
- the medical centre example raises some potentially serious privacy issues – should there be further safeguards for disclosure of an individual's sensitive health information?

⁷¹ Code, cl5(1)(c)(iii).

V Options for Reform

There is a need for reform of the Privacy Act to permit necessary sharing of personal information in the event of a large scale emergency. On a long term basis, it is not appropriate to rely on the urgent code making powers of the Privacy Commissioner. Reform will allow proposed amendments to be fully considered and debated by all relevant stakeholders. This process should consider the steps taken by Canada and Australia.

A *Australia*

1 *Federal Privacy Commissioner's reform options*

At the time of the Privacy Commissioner's review of the Privacy Act, the Commissioner recommended a number of reform options to be considered by the Australian Government, none of which were of the magnitude of the amendments that were enacted. One option was amending NPP2 to allow disclosure in times of a national emergency to a person responsible for the individual where the individual is unable to consent to the disclosure and the disclosure is:

- made for compassionate grounds; and
- is not contrary to any express wish of the individual; and
- is limited to the extent reasonable and necessary for the purpose.⁷²

Similar to the Canadian Privacy Act,⁷³ the Commissioner also suggested amending NPP2 to allow for disclosures in the public interest which “*could clearly be invoked during a large scale emergency such as the tsunami*”⁷⁴, although consideration would need to be given to whom disclosures could be made (as the Canadian provision is silent on this) as well as whether it is appropriate for a private sector organisation to be making a decision of what is in the public interest.⁷⁵

⁷² This is similar to the existing disclosure exception for health information in NPP2.4.

⁷³ Discussed at pages 24-25.

⁷⁴ *Review of Privacy Act* at 236, above n 18.

⁷⁵ *Ibid*, at 236-237.

2 Amendments to the Privacy Act

Rather than amending the current privacy principles in the Act, a new Part VIA was inserted which takes effect in the event of an emergency declaration being made. A number of issues were debated at the time of the reform process, some of which will be relevant to any reform undertaken in New Zealand.

(a) The circumstances in which a declaration can be made

The emergency declaration is made specifically for the purpose of triggering the operation of Part VIA and can be invoked in isolation of any other national emergency scheme. An emergency declaration may be made by the Prime Minister or the Minister upon being satisfied that an emergency or disaster has occurred either in Australia or outside of Australia and:⁷⁶

- it is of such a kind that it is appropriate in the circumstances for Part VIA to apply; and
- it has affected one or more Australian citizens or permanent residents (whether within Australia) or overseas; and
- if occurred inside Australia, it is of national significance “(whether because of the nature and extent of the emergency or disaster, the direct or indirect effect of the emergency or disaster, or for any other reason)”; and
- if occurred outside Australia, the Minister has consulted the Minister administering the Diplomatic Privileges and Immunities Act 1967 before making a declaration.

There was concern about the wide ranging nature of the pre-conditions, which could result in a declaration being made in circumstances not even remotely similar to a large scale natural disaster or an international terrorist situation.⁷⁷

The Federal Privacy Commissioner’s view was that the preconditions to the declaration should be more specific and referred to the approach taken in the United Kingdom where emergency is

⁷⁶ Privacy Act 1988, ss80J, 80K.

⁷⁷ These concerns were raised by the Australian Democrats, Australian Privacy Foundation and the Federal Office of the Privacy Commissioner. See also Standing Committee on Legal and Constitutional Affairs *Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006) which contained Senators Andrew Bartlett and Natasha Stott Despoja *Additional comments and points of Dissent by the Australian Democrats* at [1.11].

defined in the Civil Contingencies Act 2004 (UK) to include “*an event or situation which threatens serious damage to human welfare....*”

There is no reason to believe the Australian Government wanted to put in place a regime allowing the Prime Minister of the day to dispense with the usual privacy protections allowing easier flow of information for the government for simply any event of national significance. However, legislation must reflect its aims, and that was to address *the practical issues faced by agencies, the private sector and non-government organisations, which were highlighted during events such as the Asian tsunami in December 2004.*⁷⁸ The pre-conditions are unnecessarily wide, and if New Zealand is to amend its Act to include ‘permitted purposes’ as wide as that in the Code, then the type of emergency in which these provisions are to apply should be defined with greater certainty.

(b) Length of declaration

An emergency declaration can be for a period up to 12 months⁷⁹ and this was considered to be too long by some submitters.⁸⁰ These are emergency provisions, and not ‘business as usual’, and should facilitate the relief effort in the period immediately after the emergency, and for no longer. If, for example, a longer period is required for victim identification, there should be specific provisions dealing with this.⁸¹ Twelve months is a long time for emergency provisions, and a shorter time period should be declared where appropriate. The concern of course is that the maximum period becomes the default position.⁸² The New Zealand Commissioner had the power to issue the Code for up to 12 months,⁸³ however, issued the Code for three months which was appropriate in the circumstances. If an extension is required, the Commissioner has the power to do so.⁸⁴

⁷⁸ *Explanatory Memorandum*, at 1, above n 28.

⁷⁹ Privacy Act 1988, s80N.

⁸⁰ This was the view of the Federal Privacy Commissioner, Australian Democrats and New South Wales Council for Civil Liberties.

⁸¹ See New South Wales Council for Civil Liberties *Inquiry into the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).

⁸² The two declarations made to date have been for 12 months. (Emergency (Victorian bushfires) Declaration 2009 (No. 1), Emergency (Queensland and New South Wales floods) Declaration 2011 (No. 1).

⁸³ Privacy Act 1993, s52(2).

⁸⁴ At the time of writing, there had been no notification of an extension to the Code.

(c) Disclosure to a “*person responsible for the individual*”

The definition of ‘person responsible’ is identical to cl4(3) of the Code. The Australian Privacy Commissioner’s view was that disclosure to a person responsible should be limited to the circumstances currently provided for in NPP2.⁸⁵ If New Zealand adopts an approach similar to the Code and allows disclosures to a ‘person responsible’, the medical centre example highlights additional safeguards are needed. Consideration should be given to whether there is a requirement that disclosure is permitted only to the extent necessary for the particular purpose.⁸⁶

B Canada

Canada has two relevant pieces of federal legislation:

- the Privacy Act which sets out the way in which federal government institutions are to deal with personal information; and
- the Personal Information Protection and Electronic Documents Act (“PIPEDA”) which essentially governs the collection, use and disclosure of personal information by private sector organisations.

After the Boxing Day tsunamis, there were media reports that Federal government officials were citing the Privacy Act as a reason for not releasing the names of Canadians missing and feared dead in the disaster.⁸⁷ By releasing the names, family and friends could advise officials of those on the list who were safe. In response, the Privacy Commissioner of Canada referred to the public interest exception, which provides:⁸⁸

Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

.....

- (m) for any purpose where, in the opinion of the head of the institution,
- (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

⁸⁵ These are summarised at page 21.

⁸⁶ Similar to the requirement in HIPC, r11(3).

⁸⁷ David Fraser “Commissioner speaks up on interpretation of the Privacy Act and naming tsunami victims” (2005) <www.privacylawyer.ca>. David Fraser “Editorial urges that naming Canadian tsunami victims is in the public interest” (2005) <www.privacylawyer.ca>.

⁸⁸ Privacy Act (Canada), s8(2).

(ii) disclosure would clearly benefit the individual to whom the information relates.

In the circumstances, it would appear relatively clear that this provision is relevant and the public interest in disclosure would outweigh any resultant invasion of privacy.⁸⁹

In the private sector, the PIPEDA requires the knowledge and consent of the individual for collection and disclosure of personal information.⁹⁰ Relevantly, the Act allows disclosure without the requisite knowledge or consent where the personal information is:⁹¹

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

This is much broader than the ‘health’ exception in IPP11, including a threat to the security of an individual and does not require the threat to be serious and imminent. Importantly, this exception is linked to an emergency. This could assist in times of large scale emergencies.

Amendments to the PIPEDA are currently being considered by the House of Commons,⁹² including permitting disclosure of personal information without the individual’s knowledge or consent where the disclosure is:⁹³

(d.3) necessary to identify the individual who is injured, ill or deceased, the disclosure is made to a government institution, a part of a government institution or the individual’s next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;

Authorised representative is not defined in the PIPEDA, although a legal guardian or a person having power of attorney is an authorised representative.⁹⁴

⁸⁹ This is also the view held by the Australian Federal Privacy Commissioner, see page 21.

⁹⁰ Personal Information Protection and Electronic Documents Act (Canada), c14.3, Pple3, Sch1.

⁹¹ Personal Information Protection and Electronic Documents Act (Canada), s7(3)(e).

⁹² Bill C-29. The Bill had its second reading in the House on 26 October 2010.

⁹³ Bill C-29, s9, amending s7(3) of the PIPEDA by adding a number of paragraphs, including paragraph (d.3).

⁹⁴ Personal Information Protection and Electronic Documents Act (Canada), c14.3.6, Sch1.

Considering the proposed amendment and some examples:

- The medical centre would be permitted to disclose the medical records if it was necessary to identify the woman and her husband is her next of kin. Requiring the disclosure to be ‘*necessary*’ is an important safeguard that is not a requirement of the Code.
- The public body would not be permitted to disclose information to foreign embassies.
- Disclosures by the airline and school to family may not be permitted as release of this information is unlikely to be necessary to identify the individual.
- Disclosures by the airline and school to the Police would be permitted if it is necessary for the Police to carry out their duties in identifying the individual.

A further amendment is proposed allowing disclosure to a government institution that has made a request for the information and has indicated that:⁹⁵

(iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual, or

Unlike the Australian reform, these proposed amendments fit within the current exceptions regime of the legislation and do not require a declaration to apply. They do not go as far as the Australian provisions, or the Code, in permitting disclosure for a purpose directly related to an emergency (for example, assisting individuals to obtain repatriation, medical and health services and financial and other humanitarian assistance). However, it is likely that the current ‘health and security’ exception will allow disclosures in some of these circumstances.

⁹⁵ Bill C-29, s6 amending s7(3) of the PIPEDA by adding subparagraph (iv).

VI Summary

The Privacy Act could impede the response to a major emergency or disaster, and the Commissioner took the appropriate step and issued the Code.

Looking to the future, there is a need to reform the Act to allow for the appropriate flow of necessary personal information in times of large scale emergencies or disasters. Any such amendments must include adequate safeguards for the individual's privacy that are workable in these unusual circumstances. It was appropriate to model the Code on the Australian emergency provisions – we have relatively similar legislation, values and norms and the provisions had been subject to a democratic reform process. Whether reform of the New Zealand Act takes the same approach and inserts a new regime into the Act to apply in emergencies, or provides additional exceptions to the current IPPs, is a significant issue. Canada has taken the latter approach and the analysis indicates this has merit. It would be appropriate to consider first whether reform could work within the current IPPs.

The Commissioner's review of the operation of the Code will be invaluable in the reform process, highlighting the issues at a practical level.⁹⁶ New Zealand has an advantage in that before any reform takes place it can learn from the experiences of the operation of the Code, something Australia did not have the benefit of at the time of its reform.⁹⁷

⁹⁶ The Privacy Commissioner has indicated that a review of the usefulness and operation of the Code will occur.

⁹⁷ Any reform would have to consider the Law Commission recommendations on reform of the Act, see *Review of the Privacy Act*, above n 46.

Bibliography

Text

- Penk, Stephen and Tobin, Rosemary (eds) *Privacy Law in New Zealand* (Brookers Ltd, Wellington, 2010).
- Roth, Paul *Privacy Law and Practice* Volumes 1 and 1 (LexisNexis NZ Ltd, looseleaf edition).
- Skegg, PDG and Paterson, Ron (eds) *Medical Law in New Zealand* (Thomson Bookers, Wellington, 2006).
- Solove, Daniel J *Understanding Privacy* (First Harvard University Press. United States, 2009).

Articles

- Fraser, David “Commissioner speaks up on interpretation of the Privacy Act and naming tsunami victims” (2005) <www.privacylawyer.ca>.
- Fraser, David “Editorial urges that naming Canadian tsunami victims is in the public interest” 2005 <www.privacylawyer.ca>.
- “Christchurch earthquake death toll reaches 182” 17 March 2011 <www.stuff.co.nz>.

Other Documents

Australia

Hansard

(17 October 2006) 12 CthAPD 6

Reports

- Australian Government – Office of the Privacy Commissioner *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).
- The Parliament of Australia – House of Representatives *Privacy Legislation Amendment (emergencies and Disasters) Bill 2006, Revised Explanatory Memorandum* (2006).
- The Senate - Legal and Constitutional References Committee *The real Big Brother: Inquiry into the Privacy Act 1988* (2005).

2006 Bill

- Ambulance Service of New South Wales “*Inquiry into the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).
- Attorney General’s Department “*Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 – Issues Raised by Submissions – Attorney-General’s Department Responses* (2006).
- Australian Privacy Foundation *Re Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).
- Bills Digest no 45 2006-07 *Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).
- New South Wales Council for Civil Liberties *Inquiry into the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).
- Office of the New South Wales Privacy Commissioner *Inquiry into Privacy Legislation*

Amendment (Emergencies and Disasters) Bill 2006 (2006).

Office of the Victorian Privacy Commissioner *Inquiry into Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).

Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006.

Standing Committee on Legal and Constitutional Affairs *Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006* (2006).

Declarations

Emergency (Victorian bushfires) Declaration 2009 (No. 1) dated 11 February 2009.

Emergency (Queensland and New South Wales floods) Declaration 2011 (No. 1) dated 13 January 2011.

Canada

Bill C-29

New Zealand

Privacy Commissioner Documents

Blair Stewart File note regarding earthquake related enquiries (22 March 2011).

Email from Blair Stewart to Marie Shroff regarding the issue of a code (23 February 2011).

“Extension of Christchurch Earthquake (Information Sharing) Code” (media release, 11 March 2011).

“Information Sharing Code (Christchurch Earthquake” (media release, 25 March 2011).

Letter from Privacy Commissioner to Regulations Review Committee regarding the Code (2 March 2011).

Letter from Privacy Commissioner to Regulations Review Committee regarding the Code (11 March 2011).

Privacy Commissioner *Report by the Privacy Commissioner to the Minister of Justice supplementing Necessary and Desirable: Privacy Act 1993 Review (December 1998) – Fourth supplement to the first periodic review of the operation of the Privacy Act 1993* (2008).

Privacy Commissioner *Submission by the Office of the Privacy Commissioner on the Law Commission’s Review of the Privacy Act 1993, Stage 4* (2010).

Law Commission Reports

Law Commission *Privacy Concepts and Issues – Review of the Law of Privacy Stage 1* (NZLC SP19, 2008).

Law Commission *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4* (NZLC IP17, 2010).

Legislation

Australia

Crimes Act 1914

Privacy Act 1988

Privacy Legislation Amendment (Emergencies and Disasters) Act 2006 (Australia).

Canada

Personal Information Protection and Electronic Documents Act S.C. 2000.
Privacy Act (C P-21)

New Zealand

Canterbury Earthquake Response and Recovery Act 2010.
Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).
Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) Amendment No.1.
Civil Defence Emergency Management Act 2002.
Health Act 1956.
Health Information Privacy Code 1994.
Health Practitioners Competence Assurance Act 2003.
New Zealand Public Health and Disability Act 2000.
Privacy Act 1993.

United Kingdom

Civil Contingencies Act 2004.

Table of Cases

Duncan v Medical Practitioners Disciplinary Committee [1986] 1 NZLR 513.
Case Note 2049 1996] NZPrivCmr 7.
Case Note 30372 [2001] NZPrivCmr 15.
Case Note 5733 [2001] NZPrivCmr 16.