

New Zealand Telecommunications Based Public Alerting Systems Technology Study

December 2008

New Zealand Telecommunications Based Public Alerting Systems Technology Study

Prepared for:



Ministry for Civil Defence and Emergency Management
The Department of Internal Affairs Te Tari Taiwhenua
PO Box 5010
Wellington, New Zealand

December 2008

CAENZ is an independent think tank and research facilitator funded by grants and sponsorships. CAENZ's mission is to advance social progress and economic growth for New Zealand through broadening national understanding of emerging technologies and facilitating early adoption of advanced technology solutions.

www.caenz.com

Report Authors:

Alisha Kidd, Kevin Loasby, Gavin Treadgold, Kristin Hoskin, Kevin Chong and Scott Caldwell

Acknowledgements:

CAENZ would like to acknowledge the time and support given by the Telecommunication Carriers in contributing to this project; specifically Vodafone NZ, Telecom NZ, TelstraClear and Kordia.

We would also like to acknowledge the time and support given by product vendors, industry bodies and others:

CellCast Technologies, USA; The Cellular Emergency Alert Systems Association International Secretariat (CEASA), UK; Datasquirt, New Zealand; FESA, Australia; Rocom, New Zealand; Unified Messaging Systems, Norway; Whispir, Australia; and Jill Barclay, New Zealand Police.

Approved by:



RJ (George) Hooper

Issued: December 2008

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, or otherwise disseminated, in any form or by any means, except for the purposes of research or private study, criticism or review, without the prior permission of the New Zealand Centre for Advanced Engineering.

Copyright

©2008 New Zealand Centre for Advanced Engineering

Address for Correspondence

New Zealand Centre for Advanced Engineering
University of Canterbury Campus
Private Bag 4800
Christchurch 8140
New Zealand

Phone: +64 3 364 2478 Fax: +63 3 364 2069 E-mail: info@caenz.com

EXECUTIVE SUMMARY

This Report summarises the results of a high level technology study undertaken by CAENZ into the implementation of public alerting applications on the New Zealand telecommunications network infrastructure.

This study was commissioned by the Ministry for Civil Defence and Emergency Management (MCDEM) in response to requests by regional Civil Defence and Emergency Management (CDEM) Groups for central government guidance towards the development of a National Public Alerting System.

The objective of the study was to assess the potential constraints and barriers to the implementation of a number of identified public alerting technologies on specific New Zealand telecommunications networks; and to suggest potential pathways forward.

Key Findings

1. The supporting telecommunications infrastructure for implementing a public alerting system is largely (if conditionally) in place in New Zealand, and a wide range of telecommunications based public alerting applications are also available, primarily from overseas vendors.
2. However, a number of technical constraints were identified that could impact on the implementation process, including: constraints on the availability of technical expertise amongst and within the telecommunications carriers due to existing network rollout commitments to government; and reduced network functionality for alerting applications as a result of historical business decisions or perceived lack of market for services with potential public alerting applications, such as Cell Broadcasting.
3. Additionally, implementation of a national public alerting system will also require significant investment, the active cooperation of the telecommunications carriers and regulatory changes to address the privacy issues around a national address database, which will be central to the effectiveness of a telecommunications based public alerting system.
4. Choosing to implement an opt-in telecommunications based public alerting system could accelerate the implementation timetable by negating the need for significant regulatory changes, compared to an opt-out or compulsory system. However, participation rates for opt-in systems were found to be relatively low.
5. Public alert systems delivered across both mobile and fixed lines networks were found to complement each other in terms of 'optimal alert windows'; i.e. alerts on mobiles are more effective during waking hours and vice versa for fixed line phones.
6. While the study identified that both mobile and fixed line networks can be prone to localised congestion, mechanisms are available to mitigate their impact, including congestion control and traffic prioritisation tools or splitting lines across different exchanges. These mechanisms are being installed at the carriers' discretion.
7. For mobile networks, SMS with geo-location was identified as the most optimal mechanism currently available to deliver localised alerts. While Cell Broadcasting is a technically superior mobile network technology as it is less vulnerable to congestion compared to SMS, it will require significant investment to be deployed in New Zealand.
8. Overall, telecommunications based public alert systems should be considered as part of a wider, multi-layer emergency warning system as public alert systems share the vulnerabilities and interdependencies of the underlying telecommunications infrastructure.

Recommendations

1. The development of an overarching national "public alerting architecture" or public alerting systems framework should be undertaken before the selection of "public alerting technology applications" or systems. The public alerting framework should be standards based and sufficiently open and flexible (i.e. platform agnostic) to allow the integration of Common Alert Protocol (CAP) capable public alerting applications.

2. An open, CAP capable telecommunications based public alerting system will provide financial and operational benefits due to interoperability and use of common protocols, while allowing the selection of alerting applications to meet specific regional, technical or fiscal requirements.

The failure to develop a robust Public Alerting Framework may result in ad-hoc deployments of alerting systems that are not interoperable, and cannot be easily integrated; which, for example, may require an agency to generate multiple alerts - one for each alerting technology in use (e.g. landline, SMS). Conversely, a multi-mode alerting system which utilises a single interface to send alerts may not allow the addition of other systems to the management interface.

An alternative to having one fixed line number dataset for the alerting system would be to allow all telecommunications carriers to maintain and control their own customer database that integrates with a CAP capable user interface for CDEM. This has the advantage that carriers would not be required to share the information with any other agency and would avoid the requirement and massive expense associated with constructing and maintaining a large national dataset and related issues such as commercial sensitivity. This would require telecommunication carriers to either agree to be involved in the public alerting system or for it to be mandated.

Finally, although establishing a nation-wide alerting project is complex, it presents significant local, regional and national benefit. Without it, the likelihood of individual regions being able to implement an effective multifaceted local public warning tool is low.

3. Further to the 2008 GNS Science Report (SR2008-34) into non-telecommunications based public alerting systems, a more in-depth cost-benefit analysis should be undertaken to identify the place of telecom-

munications based alerting systems in the overall emergency management toolkit.

4. Should a rationale for the implementation of a national telecommunications public alerting framework be established, a number of parallel workstreams could be undertaken in conjunction with, or in parallel to, the development of the framework. They include:
 - a. A further assessment of the required legislative / regulatory changes to address the privacy issues around the development and operationalisation of centralised and distributed address-telephone number databases;
 - b. Developing a whole-of-government approach towards identifying user requirements for ownership and use of information in the National Address Register; allocation of costs; ensuring alignment with government IT standards, and other issues; and
 - c. Engagement with telecommunications carriers to identify protocols and constraints to the implementation of the public alert applications across their networks.
5. Finally, one applicable analogue for a suitable partnership between government and the telecommunications carriers to advance the development of a national Public Alerting System may be Research and Education Advanced Network New Zealand Limited (REANNZ), a Crown-owned company set up to establish, implement, own and operate the high-speed nationwide Kiwi Advanced Research and Education Network (KAREN) telecommunications network for the research and education sectors. One of its key objectives is to facilitate participation by multiple telecommunications sector partners so as to ensure the greatest possible flexibility for ongoing evolution. This objective applies equally to the development of a national telecommunications based Public Alerting System.

CONTENTS

Executive Summary	3
Glossary	7
1. Introduction	9
2. Project Scope and Methodology	13
3. Literature Review	13
3.1 CDEM Context	13
3.2 Public Alerting Frameworks: Risks, Vulnerabilities and Interdependencies	14
3.3 Integrated Public Alerting Systems	15
3.4 International Implementations of Public Alerting Systems	16
3.5 Emerging Mobile Technologies with Alerting Applications	17
3.6 Legislative Constraints and Support	19
4. Communications System Review	21
4.1 Fixed Line Technology	21
4.2 Mobile Network Technology	22
4.3 Industry Feedback	23
5. Internet Technologies with Alerting Applications	25
6. Discussion and Recommendations	27
6.1 Public Alerting System Framework	27
6.2 Public Alerting System Selection and Evaluation	32
6.3 Overcoming Operational Limitations	34
6.4 Immediately Available Alerting Solutions	35
6.5 Final Comments	35
References	37
Appendices	39

GLOSSARY

Access network	Base station/cell-site equipment layer
AUC	Authentication Centre
A-GPS	Assisted GPS
BTS	Base Transceiver Station
BSC	Base Station Controller
CAP	Common Alerting Protocol
CDMA	CDMA (Code-Division Multiple Access) is a type of mobile telephony network that allows analogue to digital conversion so that it can be transmitted over the air. It is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimising the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.
Device	Or mobile device, mobile handset, mobile phone – a portable telephone powered by batteries
DSL	Digital Subscriber Line
EDGE	Enhanced Data Rates for GSM Evolution
EDR	Enhanced Data Rate
EGNOS	European Geostationary Navigation Overlay Service
FM	Frequency Modulation
GMSC	Gateway Mobile Switching Centre is the MSC that determines which visited MSC the subscriber who is being called is currently located. It also interfaces with the Public Switched Telephone Network. Some manufacturers place the gateway function in the MSC therefore a dedicated GMSC isn't always required.
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	GSM (Global System for Mobile communication) is a digital mobile telephony system that is widely used throughout world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitises and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.
HLR	Home Location Register is a central database that contains details of each mobile phone subscriber that is authorized to use the core network
HSPDA	High-Speed Downlink Packet Access
HTML	HyperText Markup Language

ICE	In Case of Emergency
IP	Internet Protocol
ISP	Internet Service Provider
LBS	Location Based Service
MSAS	Multi-functional Satellite Augmentation System
MUA	Mail User Agent
MSC	Mobile Switching Centre is the primary service delivery node for mobile networks. The MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during the call and takes care of charging and account monitoring.
PSTN	Public Switched Telephone Network
RNC	Radio Network Controller
SBAS	Satellite Based Augmentation System
SMSC	A short message service centre (SMSC) is the portion of a wireless network that handles SMS operations, such as routing, forwarding and storing incoming text messages on their way to desired endpoints.
TCF	Telecommunication Carriers' Forum
TEPF	Telecommunication Emergency Planning Forum
TDD	Telecommunication Device for the Deaf
TSP	Telecommunications Service Provider
TTY	Teletype/Teletypewriter
Transmission (Mobile Network)	The transport mechanism that links mobile cell sites together. This can be done by Fibre-optic or copper cable or microwave radio.
UMTS	UMTS (Universal Mobile Telecommunications Service) is a third-generation (3G) broadband, packet-based transmission of text, digitised voice, video, and multimedia at data rates up to 2 megabits per second (Mbps). UMTS is based on the Global System for Mobile (GSM) communication standard. UMTS uses WCDMA technology, and the two terms are often used interchangeably with each other.
VLR	Visitor Location Register is a central database of mobile users from other networks that are roaming on a carrier's network.
W-CDMA	WCDMA (Wideband Code Division Multiple Access) is a third-generation (3G) wireless standard which utilizes one 5 MHz channel for both voice and data, offering high speed data transfer. It is the type of mobile networks that a large number of telecommunication carriers are moving to as it is more advanced than both CDMA and GSM.

1 INTRODUCTION

The New Zealand Centre for Advanced Engineering (CAENZ) has been commissioned by the Ministry for Civil Defence & Emergency Management (MCDEM) to undertake a high-level review into the capabilities of telecommunications technologies in New Zealand that may be used for the purpose of Public Alerts or Warnings, either prior to, or during the course of a National Emergency. It has been prepared in conjunction with a MCDEM contracted review of all public alerting options (GNS Science Report, SR2008-34).

This Report summarises the results of the study and is intended to provide the Ministry with:

- a review of both public alerting technology applications currently available, and the New Zealand fixed line and mobile telecommunications networks;
- an understanding of the opportunities, constraints and enablers that might impact on the implementation of public alerting technology applications on the New Zealand telecommunications networks; and
- recommended criteria for the selection and evaluation of public alerting technology options; and a recommended framework for an optimal, telecommunications based, National Public Alerting System.

2 PROJECT SCOPE AND METHODOLOGY

2.1 Scope

The aim of this study is to review telecommunications based technologies that may be applicable for public alert systems. The study has focused on public alerting systems that are currently available and the New Zealand fixed line and mobile telecommunications networks.

The study is intended to describe the:

- Capability of the New Zealand telecommunications infrastructure to send public alerts.
- Details of the range of public alerting technology applications currently available in New Zealand and overseas and their ability to be deployed or implemented on New Zealand fixed line and mobile networks.
- Features of public alerting technology applications that may become available in the future.
- Potential technical and engineering constraints that may impact on the deployment of public alerting technology options on the New Zealand telecommunications infrastructure, including a review of the parameters/boundaries of the public alerting framework.

The following subjects were beyond the scope of this report and have not been addressed:

- Human Factors – primarily the psychological or behavioural characteristics and nuances that must be considered when crafting specific warning or public alert messages in order to elicit the desired public responses to the warnings. This study is concerned solely with the technology options used to deliver these messages.
- The National Warning System (NWS) – this study is concerned with the technologies that will deliver public alerts to the general public from the CDEM sector, while the NWS is intended to provide alerts to the CDEM sector from MCDEM.
- Local or Regional Warning Systems – this study has not taken specific regional hazard requirements into consideration in its assessment of applicable public alerting technology applications.
- Non-telecommunications based Warning Systems – non-telecommunications based

alerting tools such as sirens and radio and television warning messages, are detailed in *An Evaluation and Decision Support Tool for Public Notification Systems in New Zealand* (GNS Science Report, SR2008-34)¹.

2.2 Methodology

The methodology for this study comprised:

1. Literature Review:

The literature review involved desk research and personal telephone interviews with New Zealand and overseas based vendors, government agencies (e.g. Australian Department of Justice) and industry organisations.

The literature review examined the New Zealand and international context for emergency management; as well as contemporary international experiences of, and thinking on, telecommunications networks based public alert systems. The literature review also examined a number of ‘market-ready’ and ‘near-to-market’ communication applications and system technologies applicable to public alerting (e.g. voice, SMS etc.), and also briefly considered features of both public alerting applications currently in development, and emerging technologies, that might be applicable to public alerting in the near future.

2. Telecommunications Networks Review:

A series of personal interviews and two workshops were held with representatives from the New Zealand telecommunications providers and industry organisations (e.g. TCF, TEPF) with the aim of identifying potential constraints and opportunities to the implementation of public alerting technology applications.

Feedback was sought from the telecommunications providers on:

- potential technical constraints and opportunities to implementation at a network level;

¹ Leonard, GS, Wright, K, Smith, WD and Johnston, DM, 2008. *An Evaluation and Decision Making Support Tool for Public Notification Systems in New Zealand*, GNS Science Report SR2008-34.

- potential policy, financial and other constraints at a strategic level;
- preferences with respect to specific public alerting applications and the underlying rationale; and,
- recommendations on potential implementation pathways, timeframes and scale of investment required.

A summary of applications is presented with key features and vulnerabilities of each current communication system,

including the underlying technology used for routing communications.

Consideration was given to new integrated systems identified in the literature review that would combine web based tools with fixed and mobile technology.

3. Components of Effective Telecommunication based Public Alerting Systems:
Consideration is given to issues associated with combining multiple communication systems into an integrated public alerting framework.

3 LITERATURE REVIEW

The literature review examined the available public alerting technologies and associated technical capabilities and performance. The literature also looked at overseas implementations of the technologies; and in particular, the implementation strategies employed and enabling factors present in different countries.

3.1 CDEM Context

New Zealand Context

Under the Civil Defence Emergency Management (CDEM) Act 2002, MCDEM is responsible for maintaining the National Warning System to issue civil defence warnings received from agencies noted as being responsible for specified hazards. National warnings must be provided by MCDEM to a range of agencies including CDEM Groups and local authorities. Regional CDEM Groups are responsible for disseminating national warnings to local communities and maintaining local warning systems. In practice, often the Regional CDEM Groups delegate this responsibility to local authorities.

Telecommunication carriers, however, are under no legislative obligations to send warnings but can be co-opted by the Emergency Services (e.g. Fire Service, Police) in an emergency situation to assist in the delivery of emergency warnings.

This project has been undertaken partly in response to requests to MCDEM from regional CDEM Groups for a telecommunication based alerting system to be implemented on a national basis.

Increased interest in public alerting systems has arisen due to recent overseas experiences (e.g. Asian Tsunami and Hurricane Katrina); and locally, to the Tongan earthquake tsunami scare in Gisborne in 2007.

A nationalised approach to public alert systems would potentially provide operational benefits through the use of common and consistent public alerting applications and financial benefits through lower training costs and

economies of scale for equipment purchases. This is particularly the case in the New Zealand CDEM environment as the country may be too small to integrate and support a multitude of regional public alerting systems within a national public alerting framework.

Recent investigations into public alerting options within New Zealand at a regional level have been reported in the following publications:

- “*An evaluation and decision making support tool for public notification systems in New Zealand*”², a 2008 GNS Science Report currently being prepared for publication.
- “*Assessment of options of hazard warning systems for the Gisborne district*”³, 2007 GNS Science Report, which reviewed current warning arrangements and developed a number of recommended options for dissemination of warnings to communities in the Gisborne district.
- “*Assessment of Auckland CDEM Group warning system options*”⁴, 2006 GNS Science Report, which developed a number of recommended options for the dissemination of CDEM warnings to potentially affected businesses and communities in the Auckland Region, so that an informed decision could be made. It also assessed New Zealand and overseas examples of best practise warning systems.

International Context

Mass public alerting through telecommunications networks has recently been subject to considerable international scrutiny. This is primarily due to the occurrence of recent high-profile natural hazard-based events such as the 2004 Boxing Day Tsunami and Hurricane

² Leonard, GS, Wright, K, Smith, WD and Johnston, DM, 2008. *An Evaluation and Decision Making Support Tool for Public Notification Systems in New Zealand*, GNS Science Report SR2008-34.

³ Leonard, GS, Johnston, DM and Saunders, W, 2007. *Hazard Warning Systems for the Gisborne District: Assessment of Options*, GNS Science Report 2007/04 72p.

⁴ Leonard, GS, Johnston, DM, Saunders, W and Paton, D, 2006. *Assessment of Auckland Civil Defence and Emergency Management Group Warning System Options*, GNS Science Report 2006/002 79p.

Katrina; and more recently, Hurricanes Gustav and Ike. Each of these events highlighted the need for appropriate, response-ready alerting systems.

Media news stories on these events have illustrated the role that mobile phones performed as a means of both informal and official alerting. The large uptake of mobile phones globally, and the role they have played during these recent events, highlight telecommunication networks as the starting point for any assessment of public alerting systems infrastructure.

National public alerting research projects are currently underway in:

- Australia;
- European Union (funded by Netherlands Government);
- USA (Gulf of Mexico states, New York City, and Greater Houston);
- United Nations;
- United Kingdom;
- Sri Lanka;
- India;
- Thailand;
- Spain; and,
- Peru.

The United Nations agency for information and communication technologies, the International Telecommunications Union (ITU) has also been quite active in this space. A key project of the ITU currently underway is an investigation into the standardisation of mobile telecommunication channels for use in cell-broadcasting, so that there is consistency between countries on which channels are reserved for alert messages. This will enable travellers who use cell broadcasting to automatically receive alert messages in other countries that use cell broadcasting.

3.2 Public Alerting Frameworks: Risks, Vulnerabilities and Interdependencies

Regardless of the public alerting technologies selected, they are likely to share number of

common characteristics with the underlying telecommunication networks, including:

a. Transmission and load factors

Any failure of network transmission assets will affect the ability of any public alerting technology application to send a public alert message. For example, infrastructure loss can create network congestion outside the areas that may be directly impacted by the specific hazard event.

Telecommunications networks are usually under heavy load when a major event occurs. Sending warning messages creates additional load, and would likely generate subsequent loading as individuals seek further official and informal information. This loading increase may extend nationally and could result in delays in further message alerts being transmitted and received.

b. Optimal Alerting Windows

Speed of transmission of the alerts is subject to the underlying network load activity. Optimal speed is achievable in the period of lowest activity, typically 12:00 midnight to 4:00 am. Telecommunications based alerting has greatest value during these sleeping hours because a large proportion of the population are not listening to standard broadcast media during this time and the phone ringtones are often capable of waking people up.

Warning messages through standard broadcast media, such as radio and television, present the greatest alerting reach during normal waking hours, particularly at key news hours, because a large proportion of the population would either be listening or have access to it during this time.

c. Public engagement and Education

A comprehensive public engagement and education programme, including regular exercises, is critical to ensuring the efficacy and effectiveness of a public alerting system. For example, establishing “message credibility” is important to ensure the alerts are taken seriously and result in the correct responses being elicited to the warnings.

Messages sent over the telecommunications network may be limited in length due to device functionality and/or transmission technology. Different communities may have different

responses to similar messages⁵, therefore the content of warning messages should be cognisant of community profiles and should be concise and/or direct the recipient to a source of more detailed information.

d. Mandatory, Opt-out, and Opt-in solutions

Opt-in solutions generally do not provide saturated coverage of the population, and historically, this has been the case in New Zealand. A proportion of the population, usually the majority, for various reasons, including privacy concerns, will not subscribe to the opt-in service and will consequently be excluded from the opt-in components of the alerting system during an alert event. Appendix 1 (Opt-in System Supporting Calculations) illustrates current opt-in statistics for opt-in warning systems in effect in New Zealand.

Opt-in warnings also require greater start-up and maintenance of public education programmes to support them than mandatory options. Mandatory or opt-out solutions are therefore preferable to opt-in solutions.

e. Alert Fatigue

Alerting for minor events may dilute responses to warnings. Public alerting projects in the USA have noted this⁶. Where the alert system was an opt-in solution, individuals were more likely to opt-out as a consequence of “alert fatigue”.

f. Alerting Frequency

Any alerting system should have the ability to retransmit messages periodically because some people may not have received the initial message or may inadvertently move into the target area during the emergency event.

g. Equipment Interface

Telecommunication based alerts must be capable of dealing with a range of complexities including answering machines, carrier based add-on services (e.g. call waiting), and call forwarding. A live test in Australia undertaken by the Victorian Emergency Services Commissioner encountered several peripheral based issues caused by these complexities⁷; for

example, the auto-dialler function of the public alert system that pushed pre-recorded alert messages to fixed line phones wasn't programmed to wait for the answer machine message to complete, resulting in the answer machine only recording part of the message.

Telecommunications technologies are also subject to rapid change and telecommunication carriers regularly replace large parts of their networks to maintain pace with these advancements. Consequently, any alerting system application will need to be ‘platform agnostic’ and mandate a standards based approach in order to maximise system flexibility and resilience.

3.3 Integrated Public Alerting Systems

Integrated alerting systems allow users to send messages over a number of communication methods (e.g. email, SMS, etc.) through a single user interface.

However, New Zealand telecommunication carriers do not currently have the capability to easily send localised messages to mobile devices. While this option is available (i.e. hardware modules are available from system vendors and third party application vendors), it does not appear to have been included their deployment plans for the near to medium term.

A number of market ready integrated public alerting systems are currently available. An initial review of available solutions was performed and is included in Appendix 2 (Emerging Technologies). However, due to the rapid pace of technology development, this information is likely to date rapidly.

The review of integrated public alert systems, although not exhaustive, has indicated that a wide range of solutions with varying strengths and weaknesses are available. However, it was also apparent that the more comprehensive systems (e.g. Cellcast & UMS) appear to be from larger, overseas markets. More information on these specific systems may be found in

⁵ Betts, R, 2006. *Community Information and Warning System – The Report of the Trial and Evaluation*, Report of the Office of the Emergency Services Commissioner, Department of Justice, Victorian Government, Australia 116p.

⁶ Martin, 2008. *Commercial Mobile Alert System First Report and Order*, Federal Communications Commission Report, Washington, DC, USA, p15.

⁷ Betts, R, 2006. *Community Information and Warning System – The Report of the Trial and Evaluation*, Report of the Office of the Emergency Services Commissioner, Department of Justice, Victorian Government, Australia 116p.

Appendix 3 (Non Opt-in Systems) and Appendix 4 (Partial and/or Opt-in Systems).

Common characteristics of integrated systems:

- Susceptible to the vulnerabilities of the underlying telecommunication's network infrastructure especially speed.
- Cost and implementation timeframes increase significantly with increased functionality.

Integrated alerting systems provide advanced functionalities such as:

- Area Manager interfaces that allow the 'geo-targeting' of alerts; i.e. polygons can be defined within a GIS based system to demarcate the area and the Area Manager Interface communicates with carriers to ensure messages are only sent to those within the polygon.
- Interactive capabilities that allow the public to respond to preset questions such as acknowledging of message receipt and requests for evacuation assistance.
- Congestion control and optimisation mechanisms that aid in assuring delivery speed and throughput.
- Predefined messages for a variety of events.
- Highly accurate databases that provide up-to-date numbers and location data.
- Multi-mode delivery.
- Delivery success measurement (real time and by report).
- Tight coupling of application and technology.
- Location based services for enabling in/out of zone reporting and re-messaging.
- Automated dialling utilising many lines or ports.
- System security and access control.

Integrated Public Alerting System options

The following systems were reviewed due either to the advanced functionality they are able to provide or the current interest in them from New Zealand CDEM Groups.

Non-opt-in integrated public alerting solutions

- CellCast

Partial and/or opt-in integrated public alerting solutions

- OPTn

- CIWS
- UMS Population Alert System
- Whispir

These systems are summarised in Appendices 3 (Non Opt-in Systems) and 4 (Partial and/or Opt-in Systems) and require further detailed investigation to determine their applicability to the Ministry's requirements.

3.4 International Implementations of Public Alerting Systems

Internationally, the implementation of public alerting system capabilities by telecommunications carriers have been supported by a variety of measures, including legislation, contractual agreements and compensation mechanisms. Table 1 summarises these measures by country.

The UK, Australia and New Zealand are countries which do not currently have legislative measures in place to support the implementation of public alert systems.

Despite the low number of countries involved in the GSM Association's study (see Table 1), it appears that the telecommunications carriers have participated voluntarily in public alerting initiatives.

Europe

The Netherlands was the first country to implement a government sponsored cell broadcasting system which demonstrated strong partnerships between the private sector carriers and government⁸. This partnership is also providing significant support to an EU project on cell broadcasting.

In addition to cell broadcasting, the Netherlands uses a feature of radio broadcasting to provide messages (such as traffic updates) via the space on radio displays that carries the station ID to deliver alert messages.

Italy has requirements beyond public alerting. Carriers are required to identify Italian citizens

⁸ 2004. Dutch Government plans mobile alert system based on cell broadcast technology. Publictechnology.net. <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=1604> and 2006. U.S. Officials Observe as Dutch Test Emergency Cell Phone Alert. Officer.com. <http://www.officer.com/article/article.jsp?id=32475&siteSection=8>

Instrument	Country	Technology	Carrier Participation	Compensation
Legislation	Finland	Any technology may be used	Compulsory	Some financial compensation
Legislation and contractual agreement	USA	Probably SMS-based (but still to be determined)	Proposed to be voluntary	Possibility of government financing
Contractual agreement	Netherlands	Cell broadcast	Voluntary	No financial compensation
Contractual agreement	Italy	SMS	Voluntary	No financial compensation
Contractual agreement	Korea	Cell broadcast	Voluntary	No financial compensation
Oral agreement	India	SMS and cell broadcast simultaneously	Voluntary	No financial compensation
Oral agreement	Malaysia	Cell broadcast	Voluntary	No financial compensation

Table 1: Public Alerting System Implementation Mechanisms [source: GSMA. 2005⁹]

in a foreign country affected by a natural disaster, contact them via a text message with a set of questions, receive and collate the responses, and provide a report to their government.

Australia

‘Public alerting’ has received a high profile in Australia in 2008, with the Australian Prime Minister and State Premiers supporting a mass public alerting project intended to be operational next year. This system is expected to provide a similar level of functionality to the CIWS system tested by the Victoria Government¹⁰.

Japan

Japan is planning to use normal ‘Cell Broadcast’ for warning and informing the public for emergencies, but is also investigating a special, additional signal in the ‘Paging Channel’ for earthquake and tsunami warnings. Japan’s tsunami risk necessitates messages to be sent very rapidly. The paging channel can sound a special alert tone to all customers within 20 seconds to indicate an imminent tsunami. In contrast, cell broadcasting will take between 20 seconds and 2 minutes.

Japan does not run a 3G network compatible to the New Zealand 3G networks but this is a

technology that could be of value in the future.

United States of America

The state of Wisconsin has implemented a cell broadcasting based alerting system since 2005.

3.5 Emerging Mobile Technologies with Alerting Applications

Advancing capabilities are presenting new opportunities beyond those of a traditional mobile phone. Internationally there are several alerting services that provide insight to future possible directions for public alerting with intelligent mobile devices.

Emerging Applications

During the Literature Review, three vendors demonstrated custom applications that hinted at the potential to produce rich applications with alerting potential that build upon the extensive technical capabilities that the newer mobile devices provide.

Rave Wireless is an application designed for campuses that incorporates a wide range of applications including: course management, course messaging, course polling, course alerts, flashcards, streaming video, in-class polling, group messaging, group polling, school email, bus tracker, broadcast alerts and a campus safety application.

SquareLoop is an alerting application that receives all alerts sent using the SquareLoop

⁹ GSM Association, 2005. *Report on Emergency Alerting and Emergency Handling Initiatives*, GSMA Report p19.

¹⁰ Betts, R, 2006. *Community Information and Warning System – The Report of the Trial and Evaluation*, Report of the Office of the Emergency Services Commissioner, Department of Justice, Victorian Government, Australia 116p.

technology, determines the location of the phone to determine if the alert is relevant, and if so display the alert to the user along with an audible alert.

Zingerang is a suite of applications available for desktops and mobile devices that allow alerts to 'travel' from device to device for a particular user. If no reply is received within a certain timeframe then the system moves the alert to the next device of the user. Zingerang is currently under a trial of emergency notifications from California's Emergency Information Service (EDIS). These alerts are provided for fire, earthquake, health, weather and other events.

The number of text messages these systems are capable of sending per minute would be based on the number agreed with the telecommunication carriers. Maximum network rates of the telecommunications carriers are discussed in Appendix 6 (System Description).

Future Capabilities

The following are capabilities of mobile devices that are currently available in the market. Over time a greater percentage of devices will support these and other advanced capabilities.

a. Support for a wide range of communications protocols

Devices capable of roaming to most global cellular networks, can connect to the Internet via a variety of protocols (both cellular and Wi-Fi), share information locally via Bluetooth, and determine location using GPS, e.g. recent mobile devices from Apple and Nokia.¹¹

b. Increasing computational ability and programmability

Mobile devices are becoming increasingly advanced, some are nearly as powerful as typical computers, but are contained in an ultra-portable profile. Custom applications for these can be developed independently of the mobile phone producers or network operators creating both commercial and public good opportunities.

c. Location-awareness

Many mobile devices now have Assisted GPS

(A-GPS) embedded in them. A-GPS provides the United States Federal Communication Commission's Enhanced 911 requirements to support emergency services needs to locate mobile, and more recently VoIP devices for emergency calls to 911.

Assisted GPS works by utilising multiple means of determining the location of the device (e.g. cells sites, Wi-Fi nodes, GPS satellites). The location information can be accessed by software, so that in theory any application can access the current location of the mobile device.

Devices that have cameras and are location-aware may create further opportunities.

d. Increased Internet accessibility

The inclusion of mobile data protocols such as GPRS, EDGE, HSDPA and Wi-Fi are enabling mobile devices to connect to the Internet via multiple methods. This has significant potential not only as an information source during emergencies, but also for interactive Internet-enabled applications.

e. Push Communications

The Research in Motion Blackberry popularised the use of 'push' communications in delivering email to a mobile device. Push generally ensures that messages are delivered quickly to the mobile device. Push is being extended to support the delivery of information other than email including events, contacts, and instant messages.

f. Using the Global Positioning System for Public Alerting

The European Space Agency has suggested modifications to the GPS system that would allow the transmission of alerts via GPS satellites. As more individuals have access to GPS devices in their cars and phones, this is likely to be a viable method for distributing alerts that compliments any telecommunication-based alerting systems.

Unfortunately, this solution would be prohibitively expensive for New Zealand to invest in on our own due to the cost of launching a geosynchronous satellite required in order to broadcast the augmented signal that could carry alerts. It may be possible to implement a regional solution – such as the South Pacific or Oceania, or even a global solution. This

¹¹ GSM 850/900/1800/1900, UMTS 850/1900/2100, GPRS, EDGE, HSDPA, Wi-Fi 802.11 b & g, Bluetooth 2.0 + EDR, Assisted GPS(A-GPS).

approach is only conceptual at this stage, and may take a number of years and international debate to reach fruition.

Examples of the application of emerging technologies in alerting are provided in Appendix 2 (Emerging Technologies).

Other Potentially Customisable Mobile Tools

The carriers were found to have some in-house tools that could be adapted for use as components of a nationwide public alerting tool:

a. Vodafone NZ Crisis Text Tool

Vodafone NZ has an SMS based web interface system, used to alert its crisis team of issues. This could be configured to give CDEM access. Some customisation and installation would be required and therefore a project would need to be established. The key benefit of this tool over standard SMS is that it is built to find the quickest path to the end user. It is only viable for up to 10,000 subscribers. It doesn't rely on the SMSC's.

b. Vodafone NZ Marketing Text Tool

Vodafone NZ has developed an in-house tool which is presently being used to send marketing messages to customers. It has a built-in transmission throttling mechanism currently set to 35 outbound texts per second.

It can import an unlimited number of subscriber numbers in a variety of formats e.g. txt, csv etc. It can also set an expiry date and if a subscriber hasn't received it within 2 hours, the text message can be dumped.

It currently has a limited life and will need additional development to extend it. This tool could be used as a public alerting tool but has not been built for this purpose.

c. Telecom eTXT and Vodafone web2TXT

eTXT™ sends text messages to a group of text capable mobile phones simultaneously. Replies can be sent back to the PC or mobile which sent the message. Once set up, eTXT™ can be used to send messages to groups or individuals from Outlook, a web browser, or from a mobile phone.

d. Text Short-codes

Text short-codes are mobile SMS services

offered by Telecom, Vodafone NZ and their third Party Service Providers. Short-codes are used to send or receive text messages. A variety of shortcode services are available, such as Air New Zealand's "TextExpress" service. To use this service, a traveller texting a flight number to '737' (the service's Text Short-code) will receive a text back from the TextExpress service with the latest flight arrival and departure information.

e. Alert to NZ Citizens Overseas or Foreign Citizens within New Zealand

In the event of an onshore incident, both Vodafone NZ and Telecom NZ have the ability to identify which overseas customers are roaming on its networks and provide that information to an authority such as MFAT. Vodafone NZ stated it would take 1-8 hours depending on how many Visitor Location Registers (VLR's) the country has, which correlates to the number of cell users in the country.

3.6 Legislative Constraints and Support

A high level investigation of relevant codes and legislation has provided insight into a number of aspects relevant to the implementation of a public alerting system.

In New Zealand, several legislative constraints exist that will need to be addressed to enable a national public alerting system to be implemented. The majority of these constraints relate to the creation and management of an appropriate database to support the telecommunications based components of a public alerting system.

Enabling Policies

New policies to facilitate the implementation of a public alerting system will need to go beyond the provisions of the CDEM Act 2002 to ensure consistent message treatment, security of information and compulsory compliance across all telecommunications carriers in an environment that avoids commercial disadvantages to any individual carrier.

The Telecommunication Information Privacy Code (2003) will be central to the process of developing appropriate enabling policies, but

other relevant legislation will include:

- Telecommunications Act 2001;
- Privacy Act 1993 No 28 (as at 01 August 2008), Public Act;
- Unsolicited Electronic Messages Act 2007;
- Telecommunication Carriers Forum Codes;
- Mobile Premium Messaging Services Code 2008;
- Telecommunications Information Privacy Code 2003; and
- SMS Anti-Spam Code 2007.

Excerpts from these documents, with commentary on relevant clauses, are included in Appendix 5 (Relevant Legislation).

Summary of Specific Considerations

The following considerations will be relevant for advancing a framework for public alerting:

- Privacy Act (1993) provisions may deem the information that is kept for the public number database as personal information (Privacy Act).
- Each new telecommunications code must have the support of 75% of TCF members (TCF Codes);
- Establishing a new telecommunications code may take several months with the cumulative effect of code drafting, reviewing, consultation, revising and ratification. (TCF Codes).
- New, amended and revoked codes must be publicly notified (TCF Codes).
- Moving a code from voluntary status into law may be required (Privacy Act).
- Data access control must be stringent (Privacy Act).
- A database should not be available for any of the TCF members except to verify the content of information that it provided (Telecommunications Act).
- Clauses in the Telecommunications Industry Codes provide for emergency conditions but have been written in the context of call information made available to emergency services at the time of an emergency. This wording could be modified to include the CDEM sector's requirements (TCF Codes).
- Any code for a public alerting system will be subject to review and approval by the Council of InternetNZ and the Board of the Marketing Association, as mandated in the SMS Anti-Spam Code.
- The Emergency Services Calling Code is currently in development and may warrant consideration for CDEM needs (ESC Code).
- Collection of personal information, compulsorily rather than voluntarily, necessitates agreement that "the interests of the individual resident or traveller are served by the collection of information that is of a personal nature to facilitate receipt of an emergency warning" (Privacy Act).
- Extending a database to include information that is not publicly available such as unlisted numbers will require approval (Telecommunications Privacy Code).
- Where information is collected directly, the collecting agency must provide information about content, purpose, recipients and agency collecting (All existing opt-in systems must be compliant) (TCF Codes).
- Access to personal information should only be granted if necessary and under strict control (Privacy Act).
- Information no longer current or required must be deleted (Privacy Act).
- Show that information collected and used is for purposes of public health and safety (Privacy Act).
- Legislation may be required to prevent subscribers from opting out (Unsolicited Electronic Messages Act, Mobile Premium Messaging Services Code).
- Spam filters may prevent receipt of warning messages. This will require that the source address(es) of emergency email and SMS messages are white listed and not black-listed (SMS Anti-Spam Code).
- Permission is required to override subscriber blocking where caller line identification is required to support emergency actions (TCF Code).
- Seek a ruling that use of a search by location / GPS is outside the meaning of reverse search key based on the intended use of the database (TCF Code, Privacy Act).

Expanded comments on the relevance and possible actions that may be required are located in Appendix 5 (Relevant Legislation).

4 COMMUNICATIONS SYSTEM REVIEW

4.1 Fixed Line Technology

New Zealand is served primarily by the “Plain Old Telephone System” (POTS) - a traditional copper wire analogue network that reaches most homes in New Zealand. There are also other technologies connecting regional exchanges. Once an analogue only system, digital telephone networks are an increasing component, although most subscribers connect via analogue circuits to the Public Switched Telephone Network (PSTN). An expanded description of fixed line technology is provided in Appendix 6 (System Descriptions).

Normal circuit switched landline voice calling, traditional fax, ADSL (broadband), and dialup internet are each delivered over a combination of the POTS copper analogue and digital networks.

Types of alerting methods over fixed line networks:

- Voice – including Interactive Voice Response (IVR).
- Fax Broadcasting.
- Email.

All fixed line alert systems require knowledge of the telephone numbers that are located in the area of interest, that is address and number are linked.

Constraints

As a result of current projects by both Telecom and TelstraClear, for example the roll out of next generation network (NGN)^{12,13} services, future public alerting over fixed line technology will become increasingly dependant on power supply.

Local number portability and Voice over IP will

increase the complexity of any process that seeks to identify numbers within a specified area because the starting digits of any given telephone number are no longer localised to a particular street, suburb, town/city or region.

These issues are not necessarily a barrier to use of fixed line options but do make it more complex. Awareness of pending network versatility has to be included in any solution design and definition of industry codes.

Due to public concerns about privacy and potential misuse of personal information, legislation may be required to support the development of a national database that links telephone numbers, physical addresses, special assistance requirements and other relevant information (and perhaps also including GPS references) to facilitate efficient delivery of a public warning message to a targeted area. The recent implementation of an Integrated Public Number Database solution in Australia¹⁴ could provide a suitable model for New Zealand to follow and adapt.

Congestion Control and Next Generation Networks (NGN)

The PSTN network is built to meet demand that might occur at the busiest hour of the busiest day for voice and data (dial-up). Load factors vary by exchange. Telecom exchanges have congestion control mechanisms predominantly based on call shedding. These are internally controlled, and manually applied where required by a 24 hour Network Operations Centre.

Only 111 and a handful of other emergency service calls are able to connect when there is network congestion. New Generation Network will offer some improvement in congestion control but the level of call prioritisation that is available in these networks is still an open question for Telecom NZ, TelstraClear can currently prioritise numbers. For call prioritisation to be effective it needs to occur on the sending and receiving networks.

¹² MED 2006. Summary of Telecom Broadband Services and NGN Infrastructure Investment Issues[source: <http://www.med.govt.nz/upload/36549/summary-telecom-broadband-services.pdf>]

Issues facing NGN and proposed standards for IP traffic management are available from <http://netlab.caltech.edu/FAST/references/new-ecn-position.pdf>

¹³ Telecom New Zealand 2005. “Telecom New Zealand and Alcatel To Implement Next Generation Network”; from <http://www.geekzone.co.nz/content.asp?contentid=5116> (NGN Network Media Commentary media release).

¹⁴ <http://www.acma.gov.au>

Similarly the threat of congestion to peak capacity and any need for priority management has not yet been made clear. The implication for a public warning system is that actual levels of performance for message delivery are unknown and some post implementation testing will be required.

Telecom NZ and Alcatel are currently building the IP Voice platform for Telecom's Next Generation Network (NGN) proof of capability to government is due mid 2009. A range of new high value services will be possible as a result¹⁵.

4.2 Mobile Network Technology

Mobile market penetration is very high in New Zealand. An overview of the New Zealand mobile market is provided in Appendix 7 (Mobile Telecommunication Market).

Phone calls are made through a mobile network by a mobile device communicating with a cell site/base station controller (BSC), which relays the communication over a radio network to a carrier's mobile switching centre (MSC), which then routes it via the mobile transmission network to the PSTN network if it is a landline number; or through another mobile carrier, or another internal MSC where it terminates at the end user, if a mobile number. Diagrammatic representations of how mobile networks work may be found in Appendix 8 (Mobile Network Configuration Diagrams).

Types of alerting methods over mobile networks:

- Short Message Service (SMS).
- SMS with Geo-Location (location-aware).
- Cell Broadcasting (Type 1) (station identification).
- Cell Broadcasting (Type 2) (broadcast messaging).
- Email.
- Fax.
- Platform Specific Application.

Mobile networks are particularly sensitive to power loss, as the infrastructure requires power to operate. Telecommunication carriers routinely employ a range of back-up power capability to mitigate this; however, in a wide spread prolonged power outage, i.e. over 24-48 hours, mobile coverage could potentially be severely degraded. This vulnerability to power loss was illustrated in the February 2004 floods when cell sites lost power in the Manawatu, and in Northland in 2007.

Constraints

Mobile networks are largely designed for peak periods with some additional capacity for emergency situations.

Mobile voice networks do not cope well with sudden extreme spikes in traffic volumes such as those that might occur for rapid-onset wide-scale civil defence events. However, slow-onset events may allow carriers to implement appropriate congestion control mechanisms prior to the anticipated peak, such as:

- implementing "half rate" measures at specific cell sites to double capacity;
- Adding hardware to cell sites to increase capacity;
- Deploying mobile "cell sites on wheels" (COWS) to temporarily increase capacity in areas with limited capacity or congested cell sites (a regular occurrence at events such as music festivals); and
- Implementing traffic prioritisation or load restriction mechanisms to limit access to radio access network in order to give priority access to first responders. In general, however, mobile telecommunication carriers have a very limited ability to prioritise voice or SMS traffic, apart from 111 calls.

Cell Broadcast is an exception to the issue of extreme spikes and is purported to work in a fully-congested network.

Another general weakness for mobile phone based alerting systems is that an alert would not always be heard by the user. At night users often either do not have their mobile phone near them or they may switch them off. At times during the day, users also turn them off or onto "silent" mode; for example, while in business meetings. Even when turned on, users

¹⁵ Telecom New Zealand 2005. "Telecom New Zealand and Alcatel To Implement Next Generation Network"; from <http://www.geekzone.co.nz/content.asp?contentid=5116> (NGN Network Media Commentary media release)

may not hear their phones for a variety of reasons; for example, phones and users may be in different rooms, background noise or muffled by a hand bag. Conversely, if someone is at home they are more likely to hear a fixed line ring given that households often have more than one phone within their home.

4.3 Industry Feedback

Through a workshop and interviews, New Zealand telecommunications carriers and emergency services, such as the New Zealand Police, have provided insights into the practicalities of applying various public alerting systems in New Zealand.

Information was provided on the technical constraints and opportunities associated with currently available or near-term communications systems that are specific to consideration of public alerting options in New Zealand.

The following summarises the feedback received:

- A nation wide public alerting system will need to be robust and resilient, which could be achieved through the implementation of a range of complementary, multi-layered alerting tools (for example, telecommunication based as well as broadcast media). It is also important to note that No system is infallible and a telecommunications based public alerting application will need to be one of a wider range of alerting tools.
- The implementation of a nation wide public alerting system will require strong government leadership and coordination due to the complexity of the implementation process and the coordination required of, and between, the national telecommunica-

tion carriers.

- Existing government-industry reference groups, such as the TCF, may preclude the need to establish a new government-telecommunication industry reference group for the implementation of a public alerting system.
- Setting and managing expectations will also be crucial.
- Telecommunication networks are optimised for “peak hour, peak period” load factors, and not for public alerting traffic during CDEM emergencies. Consequently, sufficient capacity may need to be held in reserve or be capable of being deployed rapidly during an emergency event to ensure an adequate performance level for alerting. An alternative to in-place reserve capacity may be traffic prioritisation mechanisms. These performance measures, will however, require significant investment.
- Type 2 cell broadcasting is preferable to SMS as a mobile alerting tool due to its ability to operate in a congested network.
- Public education is central to the success of any alert system, to establish message source credibility, facilitate increased public uptake and population coverage, ensure the correct responses from the public to particular alerts, etc.
- Population density in Auckland is a major issue for telecommunication based public alerting tools, particularly mobile, because of potential network congestion due to the large number of messages required to be sent over a small geographical area.
- Telecommunication carriers have existing and planned future government obligations that any alerting project implementation must consider, such as Local and Mobile Number Portability.

5 INTERNET TECHNOLOGIES WITH ALERTING APPLICATIONS

HTML Injection by Internet Service Providers

It is possible for Internet Service Providers to add/replace content in web site pages downloaded by their users. This involves modifying pages as they are downloaded by subscribers to create a high visibility banner across the top of the page notifying the subscriber of a public alert. There is potential for this technique to be used for 'public good' purposes - in this case public alerting.

To be effective, the content needs to be in a highly prominent location on any downloaded web page. In addition, as this technique needs to be applied across diverse page designs, it would probably be most appropriate to inject the public alert as a full page width banner that appears before the usual content of the webpage. It is critical that any injected public alert is displayed at the top of the page to ensure that it is visible within the web browser without scrolling.

Given the high rate of Internet usage during waking hours this could be a particularly useful tool. Local Internet service providers advise that although possible in the New Zealand context, this tool would require development. This tool would be best suited for pre-prepared messages rather than event specific alerts.

Web Browser Public Alerting Plug-ins and Extensions

This solution offers similar functionality to HTML injection but as an opt-in solution achieved through browser plug-ins. Instead of modifying the pages delivered through the ISP, a public alerting browser plug-in would modify the user interface of the browser to achieve the same result – a high-visibility alert displayed

above the web page. In an event, a message could be sent via an integrated alerting system, which would then activate the plug-in feature and display a message on those computers that have downloaded the plug-in.

This solution would be suitable for event specific alerts. A browser plug-in would source the alerts from authoritative Common Alerting Protocol (CAP) servers, and would not require any involvement from the ISP, other than to ensure that traffic is able to reach the CAP servers.

This tool could be maintained through a global consortium of interested parties as a global solution allowing all countries to benefit from the application and share costs. It would be economically inefficient to redevelop the same solution for each country. The plug-in would automatically display messages relevant to the country the computer is connected in.

SP Uploaded Banners

An alternative to HTML injection and Plug-in solutions could be to develop a memorandum of understanding with the top ten frequented New Zealand websites, whereby they upload a banner onto their site in an emergency. According to Hitwise New Zealand's July 2008 "Top 20 Websites" report, the top ten frequented websites encompassed 20% of the total traffic in New Zealand. This is a reasonable coverage of the population given the number of overall websites; for example, Trademe has on average 50,000 people online at any one time.

This would be a relatively low-cost and quick solution to implement and is arguably a more effective broadcast medium during business hours than either television or radio.

6 DISCUSSION AND RECOMMENDATIONS

The Study has found that the supporting telecommunication infrastructure to create and implement a national public alerting system is largely in place for most of the options that were investigated, apart from cell broadcasting.

The following recommendations broadly fall into two categories:

- Development of a Public Alerting Framework, which refers to the environment required to support the development of a nationally consistent approach to public alerting.
- Selection of Public Alerting System(s), which refers to specific communication products or suites of products used for public alerting.

6.1 Public Alerting System Framework

The variety of commercially available public alerting systems both here and overseas, and the rapid changes occurring in the use of communications technology suggests that Government (at least in the short term), in conjunction with stakeholders such as the TCF and the TEPF, should focus on developing a public alerting framework (i.e. a system concept that is built on standards and interoperability) which sets a minimum functional requirement for entry and participation in the system. Strong central government support may be necessary to advance the development of this framework, due to the national coverage required, potential costs involved and the role of public alerting systems as a key piece of critical infrastructure.

The failure to develop a robust Public Alerting Framework may result in ad-hoc deployments of alerting systems that are not interoperable, and cannot be easily integrated. Such a situation may, for example, require a responsible agency to generate separate and multiple alerts for each alerting technology in use (e.g. landline, SMS) and across different CDEM regions. Conversely, a multi-mode alerting

system which utilises a single proprietary interface to send alerts may not allow the integration of other systems into the management interface.

Without a framework in place for public alerting, New Zealand runs the real risk of silos of public alerting systems being implemented that cannot be integrated together in times of need to provide timely and effective public alerts, particularly when trying to send alerts to multiple regions, or nationally.

The objective of a Public Alerting System Framework therefore is to provide a standards-based approach that will lead to the implementation of a platform independent interoperable public alerting system. This is essential to enable national agencies, regional, and local authorities to adopt the public alerting communication methods that are best suited for use in their region without compromising their ability to be integrated into a national public alerting network.

As with other elements of Whole-of-Government information technology, this will require the involvement of key agencies with responsibilities around information architecture. Specifically, the Information Communication Technologies Branch of the State Services Commission, the Department of Internal Affairs Government Technology Office, the New Zealand Geospatial Office, the Ministry of Civil Defence and Emergency Management, LINZ and Local Government New Zealand would have significant roles in creating a Whole-of-Government framework for public alerting.

Fundamental Data

An integrated public alerting system will require a significant amount of fundamental information to support its operation. A base component of this will be the establishment of a public number database; either a centralised database such as the National Address register (NAR), or distributed databases within an integrated framework to allow alert messages to be sent to fixed line phones.

Currently, there are a number of different overlapping datasets of fixed line subscriber information in use, and often these are commercial and have pricing and licensing restrictions in place that may prevent individual emergency management organisations from fully utilising the same dataset.

For example, there are a number of commercial vendors, respectively, of road, phone number and addressing data such as Terralink, who currently provide the road and addressing dataset used by the 111 Communication Centres. However, sharing of this data with other emergency management agencies is restricted due to privacy legislation; while in other cases, particular agencies may choose not to license the data set due to the costs involved.

This road and addressing information is required to help take textual address information such as a landline customer's address for service – e.g. street number, road name and suburb – to enable the address to be mapped and allow spatial queries to be performed on a customer database.

111 Services

All landline providers provide limited customer information to the 111 centres. Use of this information is very restricted due to privacy concerns. Currently, the information passed to the emergency services can only be used for 111 services and cannot be used for emergency management purposes. This means that subscriber information provided to the 111 Communication Centres by the landline providers may not be applicable or utilisable for public alerting purposes. In some cases, information may even be withheld by the telecommunications companies from the 111 Communication Centres – particularly information related to confidential and withheld numbers.

Even for the 111 Communication Centres, the mapping of Caller Identification details to a location is not 100% accurate. In personal communication, New Zealand Police have advised that whilst the Caller ID mapping capability has improved from 60% to 80% of presented numbers over the past 3-4 years, the 111 Services system is still not capable of

addressing all numbers presented.

For this reason, 111 Services may not be the most optimal environment to support public alerting. However, the 111 Services are currently the best source of a location specific phone number database. The policy and legislative changes outlined previously may provide mechanisms for access to, and use of, the database by MCDEM.

National Address Register (NAR)

The failure of key Government agencies to construct a National Address Register (NAR) mid-way through 2008 suggests that an approach to construct a single national database for public alerting will be prohibitively expensive, difficult to maintain, vulnerable to privacy issues and completion risks.

The NAR was intended to provide a nationally authoritative dataset that provided road centrelines, street addressing and place name information – fundamental geo-spatial data that would form the foundation of any public alerting dataset produced. It would have been consistently used across many government agencies and local government.

The NAR tendering process resulted in three tenders that meet the tender requirements and the price range fell between \$9 million and \$48 million for conforming tender responses.

Any effort to construct a public alerting database would require either a NAR to be in place to provide an authoritative location database, or would need to build one from scratch. It could be assumed that the cost of constructing a database for public alerting purposes could cost more than \$9 million if an authoritative location database is to be constructed as part of the project. This excludes ongoing maintenance costs that would be in addition to those figures mentioned above.

There still exists a need for a comprehensive and authoritative dataset that covers roads, addressing and place names – however it is unlikely to be achieved in a manner outlined in the NAR tender.

Fundamental datasets such as the NAR

concept are still required for public alerting and these needs should be communicated to groups responsible – such as the Geospatial Executive Group, the New Zealand Geospatial Office and Land Information New Zealand (LINZ).

An Alternative Distributed Approach

An alternative to creating a large single comprehensive dataset for public alerting purposes would be the US approach, where agencies responsible for public alerting produce a geographical definition of an area (or areas) that an alert is applicable to. This geographical definition would then be packaged into the Common Alerting Protocol (CAP) format and provided to all telecommunication carriers that are part of the public alerting system. It would then be the responsibility of each telecommunication carrier to use the information contained in the CAP message to identify, using their own systems and databases, all of their own customers within the defined geographical area.

This approach would allow individual telecommunication carriers to maintain and control their own customer database, without requiring them to share this customer information with any other agency or competitor. This would avoid the requirement and significant costs associated with the construction and maintenance of a large national dataset, and minimise related issues such as commercial sensitivity.

Public Alerting Information Database

A two tier approach to the development of a national Public Alerting Information Database may provide an optimal strategy to manage the conflicting demands of information collection and verification against privacy concerns and demands. Under such an approach, general records may only require a minimum amount of personal information, while an ‘opt-in’ oriented process may also be available or could be directed to identify people with vulnerabilities or special needs, such as the aged or people in care, in order to match public alerting efforts with their particular requirements for assistance.

A suggested schema for the New Zealand public number database would include:

- public number;
- name of the customer (optional);
- address at which the number terminates;
- service location (optional);
- name of the carriage service provider;
- whether the person(s) at the address require special assistance in an emergency (optional);
- nature of assistance (mandatory if assistance is required); and
- GPS reference.

Standards and the Role of the Common Alerting Protocol

Public alerting is a problem that will involve a wide range of technologies to address specific requirements, and possibly an even wider variety of stakeholder organisations. Consequently, the most optimal way to ensure that these diverse systems can be integrated to provide a best-of-breed and fit-for-purpose public alerting system will be by mandating a standards-based approach to ensure interoperability.

The US National Science and Technology Council (2000)¹⁶ recommended that:

A standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems.

Between 2001 and 2004, the Common Alerting Protocol (CAP) was developed, and in April 2004 CAP v1.0 was approved by the OASIS Emergency Management Technical Committee¹⁷. This was updated to v1.1 within 18 months, and in September 2007 was accepted by the International Telecommunications Union (ITU) as Recommendation X.1303¹⁸.

¹⁶ US National Science and Technology Council, 2000. *Effective Disaster Warnings*, Report by the Working Group on Natural Disaster Information Systems Subcommittee on Natural Disaster Reduction.

¹⁷ <http://xml.coverpages.org/emergencyManagement.html#cap>

¹⁸ <http://www.itu.int/ITU-T/newslog/Common+Alerting+Protocol+Becomes+ITU+Recommendation.aspx>

CAP plays a pivotal role in any public alerting framework, as it is a standard that defines how alerting information is represented for communication between a wide variety of disparate information systems. CAP is, in effect, the glue that ties together a comprehensive public alerting system.

CAP has the ability to greatly simplify the management of multiple alerting systems. Generally, each alerting system vendor has a proprietary interface that is used to generate and send an alert. If multiple vendors and systems are utilised for alerting, this can make it difficult to send out alerts to multiple systems in a timely manner as the alert has to be created and sent using each alerting system interface.

Systems are now being deployed that provide a single master interface to generate a CAP message and communicates this to each alerting system that has been deployed. CAP messages can be fed into all public alerting systems, not just telecommunications based systems.

Regulatory Changes

The study has identified a wide range of policies, codes of practice and legislation that will need to be reviewed in more depth to more fully understand their implications for, and impact on, the development of a national public alerting system framework. In some cases, the modification of existing prescriptive documents (for example, the Telecommunication Codes) will be required to facilitate the drafting of new legislation and codes. While the identification of specific modifications to individual policies, Codes or pieces of legislation that might lead to the achievement of optimal public alerting outcomes was outside the scope of this investigation, such a process will need to include the following elements:

- Determination by the Privacy Commissioner on key points of the Privacy Act, such as whether the association of a telephone number with an address is regarded as personal information when the identity of an individual, family or organisation that uses the telephone number is not

part of the information record.
or

- If personal information is included, it is because the subscriber has opted to provide the information¹⁹.
- Defining the governance framework for the proposed public warning system and engagement with the TCF to establish enabling codes regarding the rules for collection, maintenance and use of information collected for the purposes of emergency management. Specifically:
 - a. Supply of customer connection information to database code;
 - b. Designate the database administering authority; and
 - c. Management and operation of public warning system database code; including storage, disposal and security;
- Consideration of the cost implications of operating codes and who pays for the service(s);
- Securing signoff from TCF members;
- Determination and ratification by the Commissioners for Privacy and Telecommunications.

Recommendations: National Public Alerting System Framework

- 1 A cost-benefit analysis will need to be undertaken to determine the cost and technical effectiveness of a telecommunication based national public alerting system as a core component of New Zealand's public alerting suite of tools for civil defence emergencies. The GNS Science Report (SR2008-34) provides a useful tool for making such comparisons.
- 2 An appropriate governance structure to provide oversight over the specification of the Public Alerting framework the implementation and maintenance of the alerting system will need to be determined. Strong leadership and coordination structures will need to be developed, and driven by central government, due to the importance of a national public alerting system as a core component of New Zealand's critical infrastructure.
- 3 Decisions will need to be made around the supporting legislation that might be required

¹⁹ Privacy Act 1993 No 28: Privacy Principle Clause 2 (g) (i)

to progress the development and implementation of the national Public Alerting framework; and the obligations they might impose on the telecommunications carriers. We note that internationally, telecommunications carrier participation in the implementation of public alerting systems has been on a voluntary basis rather than being mandated through legislation.

- 4 Potentially impeding legislation around privacy and the transmission of 'Spam' or unsolicited communications will need to be altered in order to facilitate the collection and management of information critical to meeting public alerting objectives, as well as the utilisation of that information by government agencies outside the 111 Services to contact many people at the same time.
- 5 The State Services Commission and Local Government New Zealand will need to be embedded in the development of the framework to ensure that an open and standards-based whole-of-government public alerting system architecture is both developed for, and adopted as, a government standard.
- 6 We suggest that a suitable partnership be explored between government and the telecommunications carriers to advance the development of the national public alerting system framework. One analogue for such a partnership is the REANNZ (Research and Education Advanced Network New Zealand Ltd) vehicle that was established to implement the high speed nationwide Kiwi Advanced Research and Education Network (KAREN) Network amongst New Zealand's academic, education and research community. REANNZ is the Crown-owned company set up to establish, own and operate a high-speed telecommunications network for the research and education sectors. One of its key objectives is to *"facilitate participation by multiple telecommunications sector partners so as to ensure the greatest possible flexibility for ongoing evolution"* (<http://www.karen.net.nz/about-reannz/>).

Such a partnership may provide a useful commercial platform to advance essentially a 'public good' project, should Government decide to secure voluntary participation by the carriers for the implementation of a national public alerting system, rather than legislating their participation. While a national public alerting system should be

considered as core critical infrastructure, significant goodwill will be required from the telecommunications carriers in a voluntary setting, as the implementation of the national public alerting system, even if funded predominantly by government, would require significant technical integration by the carriers into the existing telecommunications networks, as well as ongoing maintenance, in a resource and capacity constrained sector.

We suggest that in the initial stages, this discussion is advanced through the Telecommunication's Emergency Planning Forum (TEPF), in conjunction with the Telecommunications Carriers Forum (TCF).

- 7 Fundamental public datasets for public alerting should be identified and communicated to the New Zealand Geospatial Office (NZGO) so that it can be brought to the attention of the Geospatial Executive Group (GEG) and LINZ.
- 8 It is important to ascertain the range of other government and emergency management agencies would require access to any database created for the purpose of the alerting system, the specific data requirements of each specific agency, and in particular, the political, legislative and policy implications that would result from such access; for example, while access to special needs information will enable emergency services better to focus their efforts and resources to where they might be needed most in an emergency event, access to such information outside an emergency event, even if done inadvertently, may trigger unexpected consequences from a legal perspective.
- 9 Ownership and appropriate allocation of costs towards ongoing operation and maintenance programmes for any supporting database to a public alerting system will need to be determined. This information was outside the scope of this study.
- 10 A suitable protocol for retrieving public numbers for fixed line phone services that have been 'geo-coded' or pre-defined to a location will need to be investigated. While retrieval of the information can be undertaken in a number of ways (i.e. via an integrated geo-coded public number database or broker systems between the alert system and the carriers that tell the

carriers system the location the alert is to be sent to and allows the carriers system to choose the appropriate numbers within that area), the retrieval protocol must take into account the various Telecommunications Codes, relevant legislation and potentially conflicting policies that might apply. There are also existing databases managed by the carriers, such as that used for number portability, that could be extended and accessed via this or another protocol. Additionally, the scope of a number of initiatives currently being undertaken on the national location database (and managed by the New Zealand Police) could potentially be extended to provide content and types of access that support a public warning system.

- 11 Appropriate contractual arrangements will need to be entered into with the Telecommunication Carriers that ensure expectations around delivery of alert messages and liability are clear.
- 12 Further detailed investigation should be made into the adoption of the Common Alerting Protocol (CAP) as the interoperability and e-Government standard for alerting systems. This should include detailed research into deployments overseas that have utilised CAP to integrate a variety of vendors alerting systems.
- 13 The infrastructure for a Public Alerting Framework could also support and complement the National Warning System, GeoNet and other alerting systems currently in place. An investigation should be undertaken to identify, and where feasible and cost effective, align the scope of the national public alerting system with the needs of hazard monitoring agencies such as GNS, NIWA and MetService.
- 14 The national public alerting framework will need to mandate that new entrants to the national public alerting system (i.e. telecommunications carriers, public alerting application vendors, etc) meet a minimum set of standards and provide a core set of functionality. This will be necessary to minimise erosion or skewing of capabilities as new and diverse public alerting technology offerings enter the market place. At present, the Civil Defence Act in of itself is not sufficiently

compelling to enforce such a requirement.

6.2 Public Alerting System Selection and Evaluation

Following the development of the national Public Alerting System framework, including the identification of key performance criteria, the next step will be the development of a process to identify and evaluate potential public alerting systems options against the performance criteria. A range of pathways are available; including choosing an existing product, a vendor (telecommunications network, carrier or other) to develop and implement, a consortium of vendors or an independent developer or team of to build. Once the required regulatory changes are sufficiently underway, this process may be undertaken in parallel and could potentially reduce time to implementation.

A variety of integrated alerting systems have been identified that are currently available and could be implemented to allow a range of alerts to be distributed over the New Zealand telecommunications network infrastructure. Given that integrated systems are available, it would be illogical to have different systems for different communication methods unless there are specific alerting requirements that could not be met by the integrated systems. The minimum functional requirement for the integrated systems should be their ability to provide for a number of users at local, regional and national level to be able to access information and send alerts as required.

Sourcing Mobile Location Information

One of the more difficult components is a method to source the mobile device numbers within a defined alert area. Given that cell broadcasting is currently not a feasible solution over both the major carriers, SMS with geo-location would appear to be the most suitable mobile option for getting messages to mobile devices within a defined alert area at present. SMS is less desirable than cell broadcasting due to its reduced effectiveness as a result of congestion during events. However, the level of investment to enable cell broadcasting on the Telecom

network warrants further investigation before finalising a decision mobile device geo-location methods.

There are a number of other methods for identifying the location of mobile devices, which place differing loads on networks. Some are available now but the specific public alert applications examined in this study appear to be reasonably cost intensive. Significant work is also being performed by other vendors around this service who were not contacted by the study team. More detailed costings and information on integration capabilities should be sought from the vendors who could provide this technology.

A further alternative is to link a mobile number to a person's home address. This is not an optimal solution as it does not cater for times when users are not in their home area, e.g. when working or travelling. However, it is likely to reduce the cost and implementation timeframes for the alerting system.

The project has identified that the traditional alerting method of sending a text message to a mobile device might not necessarily be the only or best choice for the system. Other options such as "Cell ID" and ringing and hanging up may be desirable also. Any alerting system will need to be capable of sending alternative types of messages to cater for special needs parts of the community (e.g. a voice message to a mobile for the blind). This is really only feasible through an "opt-in" programme.

Fixed Line Phone Considerations

Fixed line phone systems are not designed for multi-point use and can quickly become congested at both the origination and termination areas. There are options to mitigate this congestion through spreading dial-out lines over a number of exchanges. A fixed line alert system would appear to be most viable for geographically small urban areas where the risk of large volumes of calls into a single exchange and consequent overloading is minimised.

User Requirement Definition

It is recommended that MCDEM undertake a project to define data and user requirements

as the next step towards defining a functional specification for a public alerting system. This project would include consultation with CDEM Groups and other agencies that could meet Privacy Act Principle 10 (d) relating to emergencies as well as the Telecommunication Emergency Planning Forum and the GAC.

The outcome of this consultation would be:

- An understanding of which agencies would want access to the system and be willing to contribute financially to its development and maintenance.
- Clear identification and agreement on what the public alerting system is trying to achieve and basic system requirements documented, e.g.
 - What volumes of people will the alerting system have to cater for e.g. is Auckland the worst case scenario, or is there a situation where a greater than regionally sized alert would have to be sent?
 - What are the acceptable population and geographic coverage levels? From a telecommunications perspective 100% is not attainable.
 - Is opt-in acceptable or part of the solution?
 - Is nationwide required or are high risk area's sufficient?
 - What functionality is mission critical and not able to be sacrificed and what is desirable?
 - What type of message needs to be sent i.e. just a tone, direction to secondary information sources or a full message?
- An appreciation of the specific data fields that would be required for any supporting database.
- Identification of specific prescriptive document requirements to enable access to the system and data for by the agencies concerned.

Selection of Public Alerting Tools

Once system functionality requirements have been established, selection of specific public alerting tools will be required. In determining the tools to be used, clear expectations of telecommunication carriers will need to be

established.

Overseas experience has demonstrated that when public alerting systems have been implemented, unanticipated complexities have frequently arisen. In seeking proposals for public alerting solutions, the prior experience of the potential providers in public alerting system implementations should be taken into consideration. Providers with previous experience may be better able to anticipate issues and more accurately forecast costs and implementation timeframes than those that have not had such experience.

The resilience of public alerting tools and their underlying infrastructure is critical. In selecting public alerting tools, careful consideration should be made that the tools selected have different risk profiles. For example, sole reliance on mobile telecommunications infrastructure would possibly present high vulnerabilities in an Auckland volcanic emergency.

Careful consideration should be given to choice of vendor and how resilient the supporting alert tool infrastructure is and any risk this may introduce. For example, if one New Zealand Telecommunications Carrier was chosen to support the tool and they were seriously impacted as part of the event, not only is the telecommunications capability for that carrier lost but the alerting tool for the other carriers also.

The following components have been identified as key elements of a robust telecommunication based public alerting system:

- Channels of delivery that enable contact with all persons in the area of concern at first alert phase and during the event.
- Integrated Public Number Database (IPND) integrated with GIS data.
- Ability to send voice and text messages.
- Ability to send cell broadcast messages (if this option is chosen).
- Ability to send voice messages through a text to voice converter.
- Ability to send emails.
- Contact database and group management

with automated update.

- System for locating mobile devices in area.
- User interface that incorporates reporting functionality including call reporting.
- Throttle management (ability to deliver messages at a rate the network(s) can manage without overload).
- Bi-directional communication as required (may be use of * and # keys).
- Message validation (component that gives the message credibility).
- Integration with other processes and agreements that support response management e.g. there may not be a need to provide evacuation assistance for an area where all residents had confirmed they did not need assistance.

Public Alerting Systems Recommendations

- 1 User requirements to be defined and a request for proposal submitted to both domestic and international alerting system providers.
- 2 A location based “non-opt-in” solution should be chosen if constraints allow, as population coverage is significantly decreased with “opt-in” solutions. However, there are opt-in solutions currently in use in some regions which have had limited success and therefore, opt-in solutions should not be discounted immediately. Should the opt-in method be preferred, the supporting infrastructure for the vendors and carriers will need to be made more resilient.
- 3 Systems should:
 - support load management;
 - operate on resilient infrastructure principles;
 - support interactive response; and
 - support multi-mode delivery for increased reach and verification.

6.3 Overcoming Operational Limitations

Domestically (June 2006 Auckland Power Issue) and internationally (July 2005 London Bombings), it has become apparent that mobile networks are prone to congestion in wide scale

events. Fixed line networks are also vulnerable to congestion. An alerting system is likely to either place or prompt the public to place significant additional load on the telecommunications networks. However, there is facility to optimise networks, prioritise calls (i.e. TelstraClear can presently and Vodafone NZ is investigating) and raise capacity. Government should consider working with the TEPF to develop improved congestion control and/or optimisation mechanisms to support an alerting system and to protect communication channels in wide-scale events.

Telecom NZ is implementing new mobile and fixed line networks. Engagement with Telecom NZ now offers an opportunity to establish expectations about public alerting and congestion control capability and have facilities for these included.

Regardless of the public alerting solutions that are selected, a strong public education programme, with both local/regional and national components, will need to be implemented. Components of public alerting will likely generate curiosity and raise privacy related questions from the public. Anticipation of this interest presents an opportunity to both address public concerns and to promote public alerting education messages without having to actively solicit widespread public attention.

6.4 Immediately Available Alerting Solutions

A number of short-term solutions that would assist in public alerting were identified during this project. Many of these could be implemented relatively easily while a more robust integrated public alerting tool is being

developed. Consideration should be given to implementing facility for:

- Sending localised public alerts via text message on the Vodafone NZ network.
- Sending alerts to foreign citizens within New Zealand on both Telecom NZ and the Vodafone NZ network;
- Uploading banners with public alerts onto the top ten frequented websites;
- Developing a protocol to upload alert banners on web-pages in an emergency event;
- Using Type 1 cell broadcasting to replace Vodafone NZ cell site names displaying on mobile devices to emergency messages.

6.5 Final Comments

In conclusion, the New Zealand telecommunications infrastructure is capable of, if not currently enabled, to support an advanced mass public alerting tool, and a range of products and development options are available.

Several decisions need to be made by central government prior to the selection of alerting applications, development of an alerting framework and implementation of an alerting system. Among the decisions are how such an initiative should be funded, allocation of costs and responsibilities, what enabling policies and legislation may be required.

Although establishing a nation-wide alerting project is complex, it presents significant local, regional and national benefit. Without it, the likelihood of individual regions being able to implement an effective multifaceted local public warning tool is low.

REFERENCES

- Betts, R, 2006. *Community Information and Warning System – The Report of the Trial and Evaluation*, Report of the Office of the Emergency Services Commissioner, Department of Justice, Victorian Government, Australia, 116p.
- Donner, J, 2007. “The rules of beeping: Exchanging messages via intentional “missed calls” on mobile phones”, *Journal of Computer-Mediated Communication*, 13(1), article 1.
- Drinnan, J, 2008. “Expanded Mobile hits snag”; *NZ Herald*, August 19, 2008.
- FESA, 2007. *State Alert Overview Presentation*, FESA Procedures, 21p.
- GSMA, 2005. *Report on Emergency Alerting and Emergency Handling Initiatives*, GSMA Report, 39p.
- Heen, K. 2008. “UMS (PAS) Population Alert System White Paper”; Unified Messaging Systems White Paper 44p.
- Klein, P, 2007. *Cell Broadcast Technology for Emergency Alert Notifications*, CellCast Technologies White paper, 11p.
- Leonard, GS, Johnston, DM, Saunders, W and Paton, D, 2006. *Assessment of Auckland Civil Defence and Emergency Management Group Warning System Options*, GNS Science Report 2006/002, 79p.
- Leonard, GS, Johnston, DM and Saunders, W, 2007. *Hazard Warning Systems for the Gisborne District: Assessment of Options*, GNS Science Report 2007/04, 72p.
- Leonard, GS, Johnston, DM, Smith, W and Wright, K, 2008. *An Evaluation and Decision Making Support Tool for Public Notification Systems in New Zealand*, GNS Science Report.
- Martin, 2008. *Commercial Mobile Alert System First Report and Order*, Federal Communications Commission Report, Washington, D.C., USA, 69p.
- Mathur, AR, Ventura-Traveset, J, Montefusco, C, Toran, F, Plag, H-P, Ruiz, L, Stojkovic, I and Levy, JC, 2006. “Provision of emergency communication messages through SBAS: the ESA ALIVE concept” in *ION GNSS 2005 Proceedings*, Long Beach, California, 2969-2975, Institute of Navigation, USA. Pdf from <http://geodesy.unr.edu/hanspeterplag/publications/> Accessed 03/08/2008.
- US National Science and Technology Council, 2000. *Effective Disaster Warnings*, Report by the Working Group on Natural Disaster Information Systems Subcommittee on Natural Disaster Reduction.
- Wood, M, 2006. *Cell@ert Technical Overview V8a*, The Cellular Emergency Alert Systems Association (CEASA) Report, 12p.

Web References

2004. “Dutch Government Plans Mobile Alert System Based on Cell Broadcast Technologies”, from <http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=1604>]
- Telecom New Zealand, 2005. “Telecom New Zealand and Alcatel To Implement Next Generation Network”, from <http://www.geekzone.co.nz/content.asp?contentid=5116> (NGN Network Media Commentary media release)
- Associated Press, 2006. “U.S. Officials Observe as Dutch Test Emergency Cell Phone Alert”, from <http://www.officer.com/article/article.jsp?id=32475&siteSection=8>
- MED, 2006. “Summary of Telecom Broadband Services and NGN Infrastructure Investment Issues”, from <http://www.med.govt.nz/upload/36549/summary-telecom-broadband-services.pdf>

“EGNOS and WAAS = modern DGPS Satellite Systems”, from http://www.environmental-studies.de/Precision_Farming/EGNOS_WAAS__E/3E.html (Map of current major SBAS coverage)

“European Geostationary Navigation Overlay Service (EGNOS)”, from http://en.wikipedia.org/wiki/European_Geostationary_Navigation_Overlay_Service (EGNOS Overview)

“Wide Area Augmentation Systems”, from http://en.wikipedia.org/wiki/Wide_Area_Augmentation_System (WAAS Overview)

Ericsson “Spatial Triggering Overview Presentation”, from http://www.ericsson.com/technology/positioning_methods/spatial_triggers.shtml

Australian Communications and Media Authority (ACMA), <http://www.acma.gov.au> (Australian Media, Radio Communications and Telecommunications Regulator)

The Cellular Emergency Alert Systems Association International Secretariat, <http://www.ceasa-int.org/>

OmniStar website, <http://www.omnistar.com/> (provider of a wide area differential GPS system)

OmniStar Australia/New Zealand satellite coverage, from <http://www.omnistar.com/grfx/maps/map-ocsat.gif>

Legislation

Telecommunications Act 2001.

Mobile Premium Messaging Services Code 2008-10-13 Telecommunications Information Privacy Code 2003.

SMS Anti-Spam Code 2007.

Unsolicited Electronic Messages Act 2007.

Privacy Act 1993 no 28 (as at 01 August 2008).

Telecommunications Carriers’ Forum (TCF) Code.

APPENDICES

APPENDIX 1: Opt-In System Supporting Calculations	41
APPENDIX 2: Emerging Technologies	42
An Advanced 'In Case of Emergency' (ICE) Application	42
APPENDIX 3: Non Opt-In Integrated Public Alerting Systems	44
Appendix 3a: UMS Population Alert System	44
Appendix 3b: CIWS	46
Appendix 3c: Alerts Message Broker (CellCast Technologies)	48
APPENDIX 4: Partial and/or Opt-In Integrated Public Alerting Systems	50
Appendix 4a: Western Australian State Alert System	50
Appendix 4b: OPTn (Rocom)	52
Appendix 4c: Whispir	54
APPENDIX 5: Relevant Legislation and Commentary	56
Appendix 5a: Telecommunications Act 2001	56
Appendix 5b: Privacy Act 1993 No 28 (as at 01 August 2008), Public Act	61
Appendix 5c: Mobile Premium Messaging Services Code 2008	67
Appendix 5d: Telecommunications Information Privacy Code 2003	68
Appendix 5e: SMS Anti-Spam Code 2007	72
APPENDIX 6: System Descriptions	73
APPENDIX 7: Mobile Telecommunication Market	79
APPENDIX 8: Mobile Network Configuration Diagrams	80
APPENDIX 9: Global Positioning Systems and Public Alerting	81
APPENDIX 10: Interviewees	82
A3M AG - Tsunami Institute, Deutschland (www.tsunami-alarm-system.com)	82
CEASA UK (www.ceasa-int.org)	82
Cellcast Technologies US (www.cellcastcorp.com)	82
Ericsson Australia	82
FESA (www.fesa.wa.gov.au)	82
Gen-i	82
Kordia	82
Rocom NZ	82
Telecom NZ	82
Telstra	82
TelstraClear	82
UMS Norway	82
Vodafone Australia	82
Vodafone Italy	82
Vodafone NZ	82
Vector Communications	82
Vodafone UK	82

APPENDIX 1: Opt-In System Supporting Calculations

Region	(A) Population (15 and over)	(B) = (A) who own a mobile	Opt-in % of mobile owners (15 and over)	(C) Dwellings	(D) % Dwellings with access to a mobile	(E) = (C) * (D)	Estimate by OPTN of number opting in	Opt-in % of (E) dwellings (at 1 unit per dwelling)
NZ		80%			74.2			
Taranaki	81,427	65,142	4.61	40,461	72.1	29,172	3000	10.28
WBOP inc Tauranga	115,063	92,050	4.35	56,376	74.8	42,169	4000	9.49
Rodney	70,304	56,243	5.33	33,444	78.2	26,153	3000	11.47

APPENDIX 2: Emerging Technologies

An Advanced 'In Case of Emergency' (ICE) Application

The combination of the capabilities discussed present some exciting opportunities in public alerting and indeed emergency management in general. One example will be outlined below. The Apple iPhone will be used as an example device due to its recent release and appeal to consumers. This should apply to any recent device that contains the capabilities similar to those highlighted above.

In recent years, the concept of having an 'In Case of Emergency' (ICE) contact stored in mobile phones has gained some official support. However, this is usually limited to just recording contact details in an address book entry and doesn't utilise the full potential of the newer mobile devices.

The release of the Application Store (App Store) for the iPhone on July 11, 2008 saw the first ICE applications provided for the iPhone. Examples include 'ICE' and 'My Emergency Info'. In addition to providing emergency contact information, these are now allowing individuals to record medical notes such as allergies, medications and conditions.

It is conceivable to take these applications a great step further and bring public alerting directly to these applications - in part creating an application that is the go-to program for an emergency for the user.

For example, an emergency application could be made Common Alerting Protocol (CAP – an xml based data format for alerting technologies) - aware, so that the device can receive CAP alerts over the Internet. An individual could subscribe to a New Zealand Alerts service run by the New Zealand Government that provides secure push distribution of New Zealand alerts in a CAP format from any central or local government agency. Upon receipt of a push alert in CAP format, the application on the device could enable the device's A-GPS function, calculate the current location of the user, and determine whether the device is within the geographical bounds of the alert as defined in the CAP message. Then, if the device is near or within the area of the CAP alert, it would alert the user.

An application should go even further though as it would be possible to embed recommended emergency actions into the application, that can then be displayed following receipt of an alert. For example, recommended general actions for particular emergency types (earthquake, flood, volcano, pandemic etc) could be included with the application. Additional specific actions for the event could be embedded in the CAP alert.

The application could be further extended to allow individuals, families and businesses to include brief plans such as family emergency plans and/or checklists to guide initial response actions. It could maintain a regularly updated database of Civil Defence centres, which would allow the application to provide guidance to the nearest centre. Ideally the New Zealand Government network service suggested above would also be able to record the status of Civil Defence welfare centres so that it could advise which facilities are open and receiving those impacted by the event.

Over time it could also support the communication of event information to authorities. For example, with appropriate standards for emergency information interchange in place, the application could allow a user to take a geo-tagged photo of a downed power pole, add a textual note, and communicate this directly to the relevant local authority (as determined by the embedded latitude and longitude within the image) so that they can review, verify, and take action as appropriate. As the image is geo-tagged, it would be able to be easily imported into a geospatially-capable Emergency Management Information System and displayed on a map.

There is significant potential for a conceptual mobile application that provides not only alerting capabilities, but also interactive and reference functions. Even if communications are not available during some events, reference information contained within the device may be useful to the affected individual in, say, providing event-specific guidance around response actions.

Client applications would need to be constructed for each major mobile device platform (Windows, Blackberry, Apple, Symbian and Palm), and standards for emergency information interchange would be utilised to transfer information over the network. There is also nothing stopping similar applications being developed for desktop operating systems so that similar alerting capabilities can be deployed in homes, corporates and government agencies in parallel using the same infrastructure and architecture.

Whilst these mobile devices are currently in the higher end of the market, it is expected that over time devices with these extensive capabilities will become more and more accessible to the general population.

Any significant alerting investments in existing network infrastructure will need to be carefully considered against investment in more advanced, intelligent, and distributed systems that fully utilise the capabilities of current and future technology.

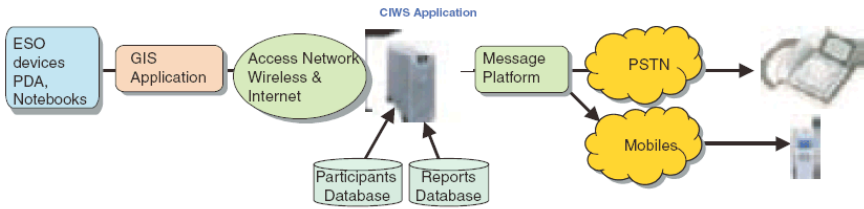
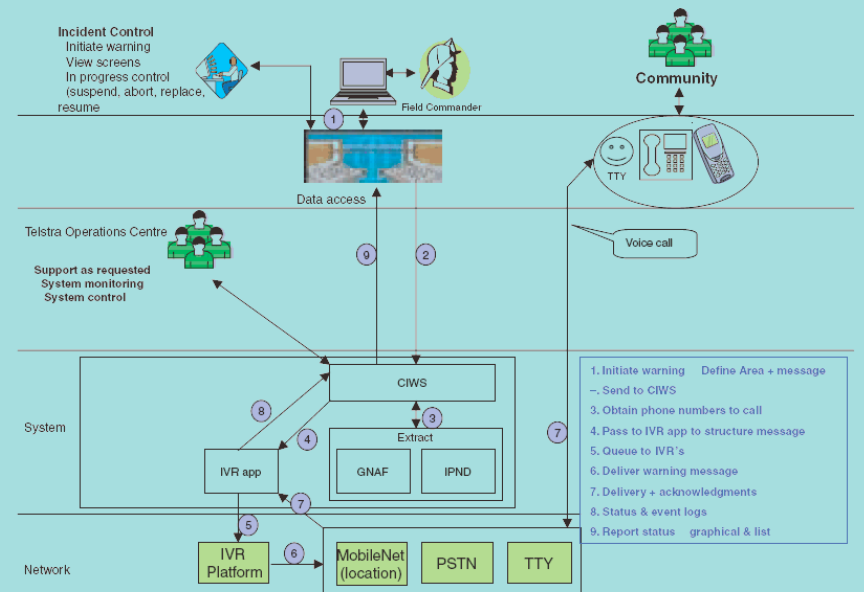
APPENDIX 3: Non Opt-In Integrated Public Alerting Systems

Appendix 3a: UMS Population Alert System

Description	<p>UMS PAS is a multi-communication channel system including fixed line, location based mobile, fax, email with radio, TV and web publishing being integrated via CAP (Common Alert Protocol). It allows geo-targeting of people (fixed and mobile) both adhoc and pre-defined via an area manager and possesses two way communication capabilities.</p> <p>The system is mainly used in Scandinavia. Their related group alert system is used by the national emergency authorities in all the Scandinavian countries (Norway, Sweden and Denmark).</p> <p>PAS uses intelligent distribution techniques to assist the sending of alert messages and protecting both the fixed and mobile network from congestion and overload. PAS can be used as a collaborative system shared among the different contributors involved in emergency situation. The profile system allows different users with different roles to have differing access to functionality.</p> <p>A range of alert messages can be pre-programmed and a selection of add-on packages can be provided:</p> <p>TAS: Traveller Alert System for identification and alert of New Zealand travellers abroad</p> <p>UAS: Underground Alert Services for identification and alert of people underground (within tunnels and subways with cell coverage)</p> <p>GAS: CDEM personnel alert system</p> <p>GIS: PAS has an integrated GIS interface. Other GIS interfaces may be integrated.</p> <p>PAS was found to be unique in that for the mobile network they install a probe within the mobile network infrastructure that retains information real time on where devices are. Therefore when an alert is required to be sent, the PAS system queries the probe for the location information of devices in the selected area. This allows quick localised sending of SMS messages. This capability was not seen in any other provider the project team reviewed.</p> <p>UMS PAS services/applications/solutions are multi-patented – including their products around the handling of congestion, localisation procedures and optimised message distribution.</p>
Infrastructure considerations	<p>The PAS system is a set of hardware, location selection is critical for its resilience. The PAS system itself has extended fail over features and load balancing mechanisms.</p> <p>UMS states that two major types of congestion can occur;:</p> <ul style="list-style-type: none">-Overload of the core network (HLR, VLR etc).-Overload of the air interface <p>Core network congestion is the more harmful one which may cause severe failure. They state that by optimisation of the SMS sending process the core network and message distribution will both be faster and far less vulnerable than ordinary SMS, allowing larger volumes and throughput.</p>
Speed	<p>This is primarily constrained by carrier infrastructure within the area,</p>

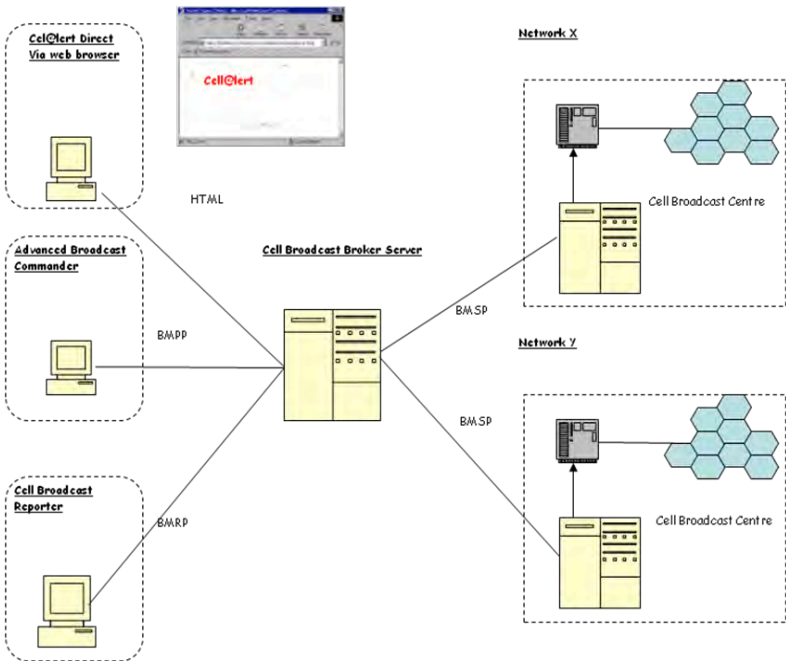
	<p>but the UMS system can provide the following:</p> <p>Voice calls: Approximately 900 voice messages pr. Minute</p> <p>Text messages: The limitation is within the air interface which has previously been discussed.</p>
Reach	<p>PAS has a high level of population coverage. For special needs areas of the public specific user groups can be created. For example hearing impaired may receive a text alert, aged a phone call, same for blind people etc.</p> <p>Tourists and visitors do not require opting in.</p>
Costs	Refer Appendix 5.
Strengths	<p>Key strengths are:</p> <p>PAS is scalable and may be used both for smaller incidents in rural areas as well as for larger incidents in urban areas/cities.</p> <p>It has a high degree of functionality and sophistication in its security and user interface including reporting on network congestion levels. Integrated congestion protection features and optimized technology for alert message distribution.</p> <p>PAS's key differentiator for New Zealand's alerting requirements is that their mobile network probe technology allows text messages to be sent to a defined area easily and quickly.</p>
Weaknesses	<p>Key weaknesses are:</p> <p>UMS believes all public initiated SMS traffic can be halted at the network layer to allow PAS messages to be sent through. However it is still subject to congestion issues at the cell site level. Therefore if the cell site layer is already congested messages may not get through. In a non-congested network it is a viable initial warning tool. A combination of this priority scheme and a radio network congestion control system may make SMS into a viable solution for public alerts throughout an event.</p> <p>The fact that this particular vendor is overseas would need to be considered for ongoing maintenance requirements.</p>
Implementation considerations	<p>UMS believe implementation timeframes once carrier acceptance has been gained and the supporting environment e.g. legislation is in place could be as little as a month.</p>

Appendix 3b: CIWS

Description	An Australian integrated fixed-line and mobile solution that is in development through the collaborative efforts of the Victoria State government, Telstra, and Ericsson. A full report on the system and its trial accompany this report. Excerpts are included here.
Infrastructure considerations	<div data-bbox="450 427 1369 725">  <p>Figure 2: Functional Blocks of CIWS Trial and Evaluation</p> </div> <p>In an operational system the participants' database would be replaced by a New Zealand equivalent of the Australian government's Integrated Public Number Database. The issue of a NZ IPND is addressed elsewhere in this report.</p> <div data-bbox="450 875 1369 1563">  <p>Figure 3: CIWS layers</p> </div> <p>A number of lines commensurate with the number of subscribers to be reached within a given time-frame are needed to deliver messages to fixed line subscribers.</p>
Speed	On one occasion during the CIWS Trial when a limited number of call out lines (20) were available, it took 60 seconds for delivery of the first message. When the number of call-out lines was increased to 61 the message delivery time was cut to 40 seconds.
Reach	National
Costs	Not available
Strengths	<p>Key strengths are:</p> <ul style="list-style-type: none"> Integrates fixed and mobile with GIS data Provides visual reporting on locations and numbers reached

	<p>Within reach for implementation and support</p> <p>Reaches all subscribers within a designated area</p> <p>Uses voice calling to reach target subscribers</p>
Weaknesses	<p>Key weaknesses are:</p> <p>The number of fixed line subscribers reached within a specified time is proportional to the number of call-out lines available and any congestion that occurs at the target exchange(s)</p>
Implementation considerations	<p>Access to an integrated public number database and the detail of information in that database</p> <p>Facilities and other infrastructure established in New Zealand</p> <p>Delivery of technology to provide geospatial data for mobile phones</p> <p>Privacy issues regarding geospatial mobile data</p> <p>Independence of system management from any single carrier</p> <p>Socio-psychological considerations regarding receipt and response to emergency messages</p>

Appendix 3c: Alerts Message Broker (CellCast Technologies)

Description	<p>The CellCast Alerts Message Broker System is a multi-communication channel system. It has an integrated web interface that allows multiple messages to be sent via a range of channels including voice, email, SMS, IM and web as well as mass scale alerting over public mobile communications systems using cell broadcast.</p> <p>The system contains an area manager function where a user can draw a polygon provided around the area they wish to target.</p> <p>For mass alerting by cell broadcast the recipient receives an SMS like text message on the screen of their phone. The phone also rings and vibrates. On board devices on the mobile could also perform text to speech translation for the blind.</p>
Infrastructure considerations	<p>The CellCast Alerts Message Broker System is a combination of hardware and telecommunications equipment that resides at a location selected by the purchaser as well as within the carriers. The Cellcast Alerts Message Broker acts as a gateway broker aggregator system and can tie in any infrastructure that the government sees as relevant from the same management system.. Messages can be received for broadcast and passed on to other systems in CAP format. Additional formats can be implemented on request.</p> <p>A diagram of a standard system is shown below.</p> <p>CellCast Alert System Configuration:</p>  <p>The diagram illustrates the CellCast Alert System Configuration. It features a central 'Cell Broadcast Broker Server' (represented by a server rack icon). To the left, three client components are shown in dashed boxes: 'CellAlert Direct Via web browser' (with a computer icon and a screenshot of the CellAlert web interface), 'Advanced Broadcast Commander' (with a computer icon), and 'Cell Broadcast Reporter' (with a computer icon). Arrows labeled 'HTML', 'BMPP', and 'BMRP' respectively connect these clients to the central server. To the right, two network components are shown in dashed boxes, labeled 'Network X' and 'Network Y'. Each network box contains a 'Cell Broadcast Centre' (server rack icon) and a hexagonal cell tower icon. Arrows labeled 'BMSP' connect the central server to each of the two Cell Broadcast Centres.</p> <p>Duplicate CellCast Alerts Message Brokers™ can be set up at geographically separate sites and connected by redundant communications methods thus ensuring a high availability rate.</p> <p>The CellCast Alerts Message Broker™ is designed to provide an interface to new technologies (e.g. 4G cellular) as they arise and uses open standard Common Alert Protocol (CAP).</p>

Speed	<p>A message can usually be created and the broadcast started in the time taken to write the message, vendor estimates less than 2 minutes. For pre-defined messages and target areas this time can be reduced.</p> <p>For time to user it depends on the message type and equipment configuration. For cell broadcast it is possible to transmit approximately 90 characters every 1.8 seconds. For mass scale public alerting by cell broadcast each message can reach an unlimited number of recipients within about 20 seconds, 32 of such messages can be sent per minute.</p>
Reach	<p>Because of the range of broadcast methods as well as the different cell broadcast channel capability it is possible to reach most sectors of the community at the same time, therefore it is socially flat. A multi language capability is provided so that non-English speakers can be catered for at the discretion of the sending authority.</p> <p>For blind people a voice message can be sent instead of a text based one, however this would have to be on an “opt in” basis. This will not necessarily be geo-specific as they may have travelled away from the area that they registered for but it will be better than not receiving the message at all. Alternatively blind people could be “opted in” to all warnings.</p>
Costs	Refer Appendix 5.
Strengths	<p>Key strengths are:</p> <ul style="list-style-type: none"> That the mobile solution works in overload situations and therefore has ongoing effectiveness through events Does not require the storing of mobile numbers Caters for a wide range of the community including those that don't speak English Fast sending rates
Weaknesses	<p>Subject to the same weaknesses as general Cell Broadcast:</p> <ul style="list-style-type: none"> Users have to enable functionality on their handset, the elderly in particular may be less inclined to do this. This would therefore require a public education programme. Not all handsets are enabled with cell broadcast functionality National standards would have to be set around emergency channels The fact that this particular vendor is overseas would need to be considered for ongoing maintenance requirements.
Implementation considerations	<p>The vendor states that it takes approximately three months for the infrastructure deployment.</p> <p>As with the other alerting systems governance structures and authorisation procedures would need to be established. CellCast can assist by engaging the various interested parties (government, telecommunications providers, system vendors) to set the terms of the Memorandum of Understanding while CellCast subsequently programs them as admission rules in the CellCast Alerts Message Broker™</p>

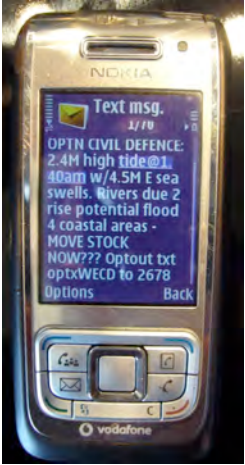
APPENDIX 4: Partial and/or Opt-In Integrated Public Alerting Systems

Appendix 4a: Western Australian State Alert System

Description	<p>The Fire and Emergency Services Authority of Western Australia (FESA) and the Western Australian Police collaborated to develop a public warning system with an independent developer, OVIS. It is a web based system capable of transmitting voice and/or text messages via landline, mobile phone, email and fax. It is a free service to the community and all publicly listed telephone numbers in the phone book are automatically registered in the database. Anyone with an unlisted number or who wants to receive StateAlerts via the alternative methods can register via a website or call centre. Three registrations are allowed per address.</p> <p>The public register their mobile number against their home address, so they can receive alerts about their home area to their mobile phone. This is not a fully localised solution, in that if the user goes out of their home area they will not receive information on the area they are within currently.</p> <p>As with most of the other systems that offer voice services it has an integrated voice recording function. It has an Area Manager function that allows target areas to be defined from the size of a suburban block to as large as a local government district.</p> <p>System specifics:</p> <ul style="list-style-type: none"> Voice messages of up to two minutes SMS maximum of 160 characters Email/fax maximum of 1000 characters Will leave messages on answering machines Will call each number up to three times <p>It has been in development for two years and has undergone user testing in a live trial. The system is ready for implementation and public launch but has to wait until privacy legislation around phone number use is changed.</p>
Infrastructure considerations	Dependent on how it is implemented in the New Zealand context and the underlying New Zealand telecommunications infrastructure.
Speed	40,000 messages in 15 minutes in normal conditions.
Reach	Dependent on how it is implemented in the New Zealand context but subject to the same reach issues as discussed under SMS and voice technology.
Costs	FESA owns the software rights and therefore would be happy to work with the New Zealand government to establish a purchase agreement.
Strengths	<p>Key strengths are:</p> <p>Development and testing has been completed and therefore implementation timeframes would not be considerable.</p>
Weaknesses	<p>Key weaknesses are:</p> <p>The opt in solution for mobiles reduces the population coverage.</p> <p>Maintenance support would be from an overseas provider however a relatively close one.</p>
Implementation	Implementation timeframes once an agreement has been come to and

considerations	the supporting environment is in place would not be significant.
----------------	--

Appendix 4b: OPTn (Rocom)

Description	<p>OPTn is an SMS based service provided by Rocom. It has a web based user interface that allows text messages to be sent to users that “opt in” to receive the service on their mobile phone.</p> <p>Standard SMS message characteristics apply of the alert being received as per the user’s settings e.g. vibration, sound and 160 characters in each alert. More characters can be rolled into a subsequent message. The picture below shows how a message might look.</p>  <p>Members can opt in automatically by texting the appropriate code to OPTn and manually either by phoning an 0800 number, on the web or faxing Rocom. They have a large number of schools that are collecting parent’s numbers and on-sending them, Civil Defence offices are also collecting numbers. A variety of methods to opt in are required as some users such as the elderly do not like to text. For manual registrations Rocom need to physically enter the mobile phone numbers into the system.</p> <p>This service is available in New Zealand and Australia with seven councils in NZ using the OPTn service, with Waitakere City Council and Northshore City Council soon to join.</p> <p>Pre-programmed messages are possible but it would need Telecommunication provider setup and approval. Single level authentication is provided.</p> <p>Rocom states they could develop a fixed line tool relatively easily as it is very similar technology. Rocom estimated it would cost under \$100,000. For this service each council would have to further delineate code boundaries within their area up to a level of granularity that they wanted to be able to bound their alerts to.</p>
Infrastructure considerations	<p>OPTn is a series of databases relating to an area code e.g. Lahar or RD CD (Rodney district civil defence) on highly available servers currently hosted by iServe in Wellington NZ. These databases are connected to the Rocom SMS Gateway (GiMP) hosted in Datacom, Auckland, NZ. The gateway is directly connected over Datacom’s permanent data links with the NZ mobile carriers to deliver the SMS alert to mobile users who have “opted –in”.</p> <p>Both the OPTn servers and the SMS gateway are single points of failure. Rocom is currently looking at bringing the Wellington server to Datacom in Auckland and also having a Technology Recovery system</p>

	offshore.
Speed	<p>The carriers (Vodafone and Telecom) currently govern the GiMP's throughput to 10-15 messages per second, 600 messages per minute, 36,000 per hour. The GiMP has the ability to send 185 per second per server.</p> <p>This could be boosted with the agreement of the carriers to the carrier's maximum.</p> <p>Time required to access the system and send an alert message is minimal.</p>
Reach	Rocom estimates that 98% of mobile phones currently in use can receive text messages. Internal or overseas visitors would need to opt in to the service to receive it.
Costs	<p>Opting in and out is free to the user. Rocom currently charges Councils \$25 per month with SMS costs at 15c per SMS sent. If it is to be used as a national public alerting tool Rocom suggests building better redundancy, interfacing with Government systems, reporting functionality etc... Their broad estimates would be in the range of NZD\$100,000 to \$200,000.</p> <p>With the additional redundancy maintenance costs are estimated at \$4-7000 per month which could be split between MCDEM and the Civil Defence Emergency Management Groups.</p>
Strengths	<p>Key strengths are:</p> <p>A number of areas are currently using the OPTn service with some public having already received an SMS from Civil Defence. This creates a level of familiarity by the councils and the public.</p> <p>Technical support is based in New Zealand</p> <p>They have a long history and experience of working with the New Zealand telecommunication carriers.</p> <p>Emergency Managers can also send a text to the public from their phone.</p>
Weaknesses	<p>Key weaknesses are:</p> <p>Subject to the same weaknesses as general SMS.</p> <p>The areas around NZ must be divided into codes. This does however provide traffic management and helps to ensure that the people first affected will receive the alert. This is a preventative congestion control measure only and does not stop congestion from occurring if all users decided to call/text each other.</p> <p>Having the public opt in to the service reduces population coverage.</p> <p>Emergency managers can currently send messages from their mobile phone, which if the phone is stolen could be used maliciously. This functionality could be turned off.</p>
Implementation considerations	<p>Government would need to define the areas and codes for the system. This could be done relatively easily using existing council boundaries. Significant amounts of public education would be required to get sufficient levels of population coverage.</p>

Appendix 4c: Whispir

Description	<p>Provided by an Australian based company, Whispir is a 'high availability messaging platform' that enables the instant and automatic invocation of communications across email, SMS, web and voice channels, from any location including from a mobile phone.</p> <p>Provided as a managed service, this wireless and web-based communication management system facilitates invocation, collation, distribution and delivery of communications during an incident or crisis without having to install or maintain any software or hardware.</p> <p>It has a user friendly interface and advanced message tracking and reporting features to monitor message delivery and response in real time. Text can be turned into voice and automated voice calls sent. Teleconferences can be invoked with a call out process removing the need to dial long numbers and remember account codes and pins.</p> <p>Flexible message templates for pre-approved communications are able to be input. It has rules based message escalation processes e.g. it send messages automatically to a person's alternate if they do not respond to a message within a pre-defined time frame.</p> <p>It utilises message delivery reports to manage communications by exception. Reports available in real-time that provide a complete record of all communications in a single location for all communication methods.</p> <p>Opt-in subscription interfaces are available for subscription services if desirable in certain circumstances. Customer information data tables reside in Whispir's hosted in data centres, containing the hardware, software, data and networking, upgrades, and maintenance in a fully managed, secure environment. Clients are responsible for managing their own data</p>
Infrastructure considerations	An edge-of-network IP based fully hosted solution.
Speed	Standard configuration up to 3000 messages per minute. Optimised configuration with telecommunication carrier integration up to 5000 messages per second.
Reach	Equivalent to standard voice and SMS.
Costs	Refer Appendix 5.
Strengths	<p>Key strengths of the Whispir system are:</p> <p>Whispir has several years experience in Australia and is rapidly expanding into the New Zealand market, therefore it has or will have shortly knowledge and experience of working with local telecommunication carriers.</p> <p>User friendly interface and advance reporting over a number of communication methods.</p> <p>It has advanced API's that enables integration of the Whispir platform with other systems.</p> <p>It supports advanced teams and distribution list management incorporating time profiles, recipient defined message preferences and escalation.</p> <p>Capacity planning ensures that service level obligations are met.</p> <p>Can send alerts from a mobile phone.</p>

Weaknesses	<p>Key weaknesses are:</p> <p>Infrastructure and maintenance teams not currently held within New Zealand, therefore reliant on Southern Cross cable and support teams coming from Australia. Whispir is looking to resolve this in the next 6 months.</p> <p>Whispir does not currently provide mass public alerting capability i.e. it still needs to be integrated with:</p> <p>A location area manager (Whispir has developed but is not in use with any clients as yet)</p> <p>A fixed line number database (Primarily Government's responsibility)</p> <p>A way of locating mobile phone numbers in an area (Still required)</p>
------------	---

APPENDIX 5: Relevant Legislation and Commentary

Appendix 5a: Telecommunications Act 2001

Sections of the Telecommunications Act included here describe the processes used to invoke a new code and amend or remove an existing one. Sections describing the process for the Commissioner to create a code have not been included. Where appropriate, explanatory comments have been provided

Section	Comment
Schedule 2 - Telecommunications access codes s 7(2) 1 Telecommunications access codes prepared by Forum This heading was inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).	The Forum referred to here is the Telecommunication Carriers Forum (TCF)
1 Forum may prepare code (1) The Forum may, on its own initiative or if invited to do so by the Commission, prepare 1 or more telecommunications access codes for approval by the Commission. (2) The Commission may issue guidelines to the Forum on any matters relating to telecommunications access codes, including advice on what matters are appropriately dealt with by those codes. Subclause (2) was inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).	The TCF, rather than the Commissioner, would likely be engaged in the preparation of a code to provide the information required to sustain a public warning system.
Requirements for draft codes for designated access services and specified services (1) A draft code for 1 or more designated access services or specified services may only provide for procedures, requirements, and other matters, not inconsistent with this Act, that relate to an aspect or aspects of the supply of that service or those services. (2) A draft code to which subclause (1) applies must— (a) be consistent with applicable access principles and any regulations made in respect of the applicable access principles; and (b) be consistent with the purpose set out in section 18; and (c) comply with the Commerce Act 1986; and (d) not directly provide for the implementation of initial and final pricing principles and any regulations relating to those principles. Subclause (1) was substituted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).	
Requirements for draft codes for designated multi-network services (1) A draft code for 1 or more designated multi-network services may only provide for procedures, requirements, and other matters, not inconsistent with this Act, in respect of— (a) the functions that must be performed by a system for determining the service; (b) the standard to which those functions must be performed. (2) A draft code to which subclause (1) applies must— (a) be consistent with the purpose set out in section 18; and (b) comply with the Commerce Act 1986; and (c) not directly provide for the apportionment of the cost of delivering the service between the access seeker and all access providers of the service.	
3A Requirements for draft codes for services supplied under registered undertaking (1) A draft code for 1 or more services supplied under a registered undertaking may only provide for procedures, requirements, and other matters, not inconsistent with this Act, that relate to an aspect or aspects of	The code for provision of number –location data will comply with this section and not require the provision or disclosure of any commercial or pricing

Section	Comment
<p>the supply of that service or those services.</p> <p>(2) A draft code to which subclause (1) applies must—</p> <p>(a) be consistent with the purpose set out in section 18; and</p> <p>(b) comply with the Commerce Act 1986; and</p> <p>(c) not provide for any matter relating to the price of the service.</p> <p>Clause 3A was inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	<p>information.</p> <p>Rigour is required in establishing the security of a compiled database so that it is unavailable in its entirety or part thereof for any of the TCF members except to verify the content of information by a member of the information that it provided.</p>
<p>Forum must arrange referendum on draft code</p> <p>(1) Before a draft code is submitted to the Commission for approval, the Forum must hold a referendum on the draft code.</p> <p>(2) The Forum must take all practicable steps to invite, for the purpose of voting on a draft code, all eligible persons who are, in the opinion of the Commission, affected or likely to be affected by the draft code.</p> <p>(3) The Forum may otherwise determine the way in which the referendum is conducted.</p> <p>(3A) All eligible persons who are, in the opinion of the Commission, affected or likely to be affected by the draft code may vote in the referendum.</p> <p>(4) The following persons are entitled to register with the Commission as eligible persons:</p> <p>(a) a person who provides a telecommunications service by means of some component of a PSTN or PDN that is operated by that person;</p> <p>(b) an access seeker or access provider of—</p> <p>(i) a designated service or specified service; or</p> <p>(ii) a service supplied under a registered undertaking;</p> <p>(c) any other person whom the Commission determines has a material interest in a draft code because that person is about to become, within the foreseeable future, a person referred to in paragraph (a) or (b).</p> <p>(5) A person entitled to register with the Commission under subclause (4) may be a member of the Forum for the purposes of this Act.</p> <p>Subclauses (2) and (3) were substituted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p> <p>Subclause (3A) was inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p> <p>Subclause (4) was substituted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	<p>This section speaks to the process that any new code will have to endure in order to be approved and applied.</p>
<p>Draft code may be submitted to Commission</p> <p>The Forum may submit to the Commission a draft code, along with a statement—</p> <p>(a) that identifies the designated service or specified service to which the draft code applies; and</p> <p>(b) that identifies every relevant applicable access principle; and</p> <p>(c) that the draft code meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require); and</p> <p>(d) that either the draft code—</p> <p>(i) has the support of all eligible persons who voted on the draft code; or</p> <p>(ii) is supported by at least 75% of eligible persons who voted on the draft code; and</p> <p>(e) that identifies any cost implications in relation to the draft code; and</p> <p>(f) that indicates how any cost will be apportioned between eligible persons to whom the draft code applies; and</p> <p>(g) that sets out how the apportionment is consistent with the purpose set out in section 18.</p> <p>Paragraph (c) was amended, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p>	<p>Consideration should be given to the cost (e) of operating the code to provide the necessary information.</p> <p>MCDEM may wish to discuss this with MED. MED are currently guiding the work of the TCF to develop a code entitled “Emergency Services Calling Code”</p>

Section	Comment
Paragraph (d) was substituted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).	
<p>6 Commission must consider whether consultation on draft code is needed</p> <p>(1) The Commission must make reasonable efforts to consider whether or not consultation on the draft code is needed not later than 10 working days after the date on which the Commission received the draft code.</p> <p>(2) The Commission need not do any of the things set out in clause 7(1) if the Commission is satisfied that the Forum has—</p> <p>(a) published a notice of the draft code, or caused a notice of the draft code to be published, in the Gazette; and</p> <p>(b) at all reasonable times, made the draft code available for inspection on the Forum's website in an electronic form that is publicly accessible; and</p> <p>(c) included in the notice of the draft code the closing date for submissions, which must not be later than 20 working days after the date of giving the notice in the Gazette; and</p> <p>(d) given to the Commission copies of all submissions on the draft report.</p>	
<p>7 Consultation process on draft code</p> <p>(1) Immediately after the Commission considers that consultation on the draft code is needed, the Commission—</p> <p>(a) may request the Forum to consult with any person or group specified by the Commission;</p> <p>(b) must consult with every eligible person who has voted against the draft code; and</p> <p>(c) must give public notice of the draft code.</p> <p>(2) A person is entitled to make submissions to the Commission not later than 20 working days after the date on which public notice of the draft code is given.</p>	Sufficient time, probably months, should be allowed for the consultation and submission process.
<p>Variation of draft code</p> <p>(1AA) This clause applies if the draft code has been prepared by the Forum under clause 1.</p> <p>(1) The Commission must make reasonable efforts to consider whether or not the draft code meets all of the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require) at least 20, but not later than 40, working days after the closing date for submissions under clause 7(2).</p> <p>(2) If the Commission considers that the draft code does not meet all of the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require), the Commission—</p> <p>(a) must not approve the draft code; and</p> <p>(b) must return to the Forum the draft code, along with the Commission's reasons why the draft code does not meet a particular requirement; and</p> <p>(c) must, if the draft code does not comply with the Commerce Act 1986, advise the Forum that an authorisation granted by the Commission in accordance with that Act is needed before the draft code may be approved under this Act.</p> <p>(3) If the Forum resubmits the draft code to the Commission, clauses 1 to 7 and subclauses (1) and (2) again apply to the resubmitted code.</p> <p>Subclause (1AA) was inserted before subclause (1), as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p> <p>Subclauses (1) and (2) were amended , as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p>	
<p>When Commission must approve draft code</p> <p>[Repealed]</p> <p>Clause 9 was repealed, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	

Section	Comment
<p>10 Commission's discretion to approve draft code</p> <p>The Commission may approve a draft code if the Commission is satisfied that—</p> <p>(a) the draft code meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require); and</p> <p>(b) all the consultation referred to in clause 7(1) has been carried out; and</p> <p>(c) [Repealed]</p> <p>Paragraph (a) was amended, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p> <p>Paragraph (c) was repealed, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	
<p>Commission must refuse to approve draft code in certain cases</p> <p>Despite clauses 9 and 10, the Commission must refuse to approve a draft code if it is satisfied that the draft code deals with a matter that is more appropriately dealt with in—</p> <p>(a) a determination under section 27; or</p> <p>(b) a standard terms determination under section 30M; or</p> <p>(c) a designated multinet service determination under section 39.</p> <p>Clauses 10A and 10B were inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	
<p>10B Amendment of draft code</p> <p>(1) This clause applies only if the Commission considers that, because of a change in circumstances, a draft code submitted to it no longer meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require).</p> <p>(2) The Commission may prepare, or request the Forum to prepare, a specific amendment to the draft code to ensure that it meets all of those requirements.</p> <p>(3) If the Commission prepares the amendment, the Commission must—</p> <p>(a) ensure that the consultation referred to in clause 7(1) has been carried out on the amended draft code; and</p> <p>(b) decide, as soon as practicable after paragraph (a) has been complied with, whether to approve the amended draft code under clause 10.</p> <p>Clauses 10A and 10B were inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	
<p>11 Expiry of approved code</p> <p>(1) An approved code expires, in whole or part (as the case may be), on the revocation of the relevant applicable access principle.</p> <p>(2) An approved code expires on the revocation or expiry of the designated service or specified service to which the approved code applies.</p>	
<p>12 Revocation of approved codes</p> <p>(1) The Commission must, on the request of all eligible persons, revoke an approved code.</p> <p>(2) The Commission may revoke an approved code if—</p> <p>(a) requested to do so by 75% of eligible persons who voted on the approved code; and</p> <p>(b) the Commission considers that, because of a change in circumstances, an approved code no longer meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require).</p> <p>(3) Despite subclause (2), the Commission may revoke an approved code if it is satisfied that to do so best gives, or is likely to best give, effect to the purpose set out in section 18.</p> <p>Subclause (2)(a) was substituted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p> <p>Subclause (2)(b) was amended, as from 22 December 2006, by section 57</p>	

Section	Comment
<p>Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p> <p>Subclause (3) was inserted, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83).</p>	
<p>Amendment of approved codes</p> <p>An approved code may be—</p> <p>(a) amended in the same manner that it was approved; or</p> <p>(b) amended by the Commission in accordance with clause 14.</p>	
<p>Amendment of approved code initiated by Commission</p> <p>This clause and clause 13 apply only if the Commission considers that, because of a change in circumstances, an approved code no longer meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require).</p> <p>The Commission may request the Forum to prepare a specific amendment to an approved code for submission to it within a specified time.</p> <p>If the Forum complies with the Commission's request under subclause (2), the same procedure that applies to draft codes must be followed.</p> <p>Subclause (1) was amended, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by substituting the word “clause” for the word “section”.</p> <p>Subclause (1) was amended, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p>	
<p>15 Consequences of not complying with Commission's request under clause 14(2)</p> <p>(1) If the Forum does not comply within a reasonable period with the Commission's request under clause 14(2), the Commission may prepare the amendment.</p> <p>(2) If the Commission prepares the amendment, the Commission must—</p> <p>(a) ensure that—</p> <p>(i) the amendment meets all the requirements set out in clause 2 or clause 3 or clause 3A (as the case may require); and</p> <p>(ii) the consultation referred to in clause 7(1) has been carried out; and</p> <p>(b) approve the amendment as soon as practicable after paragraph (a) has been complied with.</p> <p>Subclause (2)(a) was amended, as from 22 December 2006, by section 57 Telecommunications Amendment Act (No 2) 2006 (2006 No 83) by inserting the words “or clause 3A” after the expression “clause 3”.</p>	
<p>16 Public notice of approved codes</p> <p>The Commission must give public notice of—</p> <p>every approved code; and</p> <p>every revocation of an approved code.</p>	

Appendix 5b: Privacy Act 1993 No 28 (as at 01 August 2008), Public Act

Section	Comment
<p>4 Actions of, and disclosure of information to, staff of agency, etc</p> <p>For the purposes of this Act, an action done by, or information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of the person's employment shall be treated as having been done by, or disclosed to, the agency.</p>	<p>If the agency is MCDEM then one person at MCDEM having received personal information is deemed to have received it on behalf of all of MCDEM</p>
<p>6 Information privacy principles</p> <p>The information privacy principles are as follows:</p> <p>Information Privacy Principles</p> <p>Principle 1 Purpose of collection of personal information</p> <p>Personal information shall not be collected by any agency unless—</p> <p>(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and</p> <p>(b) The collection of the information is necessary for that purpose.</p>	<p>Agreement is needed that the interests of the individual resident or traveller are served by the collection of information of a personal nature in order to facilitate receipt of an emergency warning.</p> <p>See principle 10 (d)</p>
<p>Principle 2 Source of personal information</p> <p>(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.</p> <p>(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—</p> <p>(a) That the information is publicly available information; or</p> <p>(b) That the individual concerned authorises collection of the information from someone else; or</p> <p>(c) That non-compliance would not prejudice the interests of the individual concerned; or</p> <p>(d) That non-compliance is necessary—</p> <p>(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or</p> <p>(ii) For the enforcement of a law imposing a pecuniary penalty; or</p> <p>(iii) For the protection of the public revenue; or</p> <p>(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or</p> <p>Principle 2 subclause (2)(d)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word "tribunal" for the word "Tribunal".</p> <p>(e) That compliance would prejudice the purposes of the collection; or</p> <p>(f) That compliance is not reasonably practicable in the circumstances of the particular case; or</p> <p>(g) That the information—</p> <p>(i) Will not be used in a form in which the individual concerned is identified; or</p> <p>(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or</p> <p>(h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.</p>	<p>2 (a) Information that is publicly available would include a] directories and b] property information</p> <p>Omissions for a] will include all unlisted numbers and for b] all instances where the property owner has invoked the option to suppress property owner details in on-line property descriptions.</p> <p>2 (g) (i) begs a decision by the Privacy Commissioner on whether the association of a telephone number with an address is regarded as personal information when the identity of an individual, family or organisation that uses the telephone number is not part of the information record.</p>

<p>Principle 3 Collection of information from subject</p> <p>(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—</p> <p>(a) The fact that the information is being collected; and</p> <p>(b) The purpose for which the information is being collected; and</p> <p>(c) The intended recipients of the information; and</p> <p>(d) The name and address of—</p> <p>(i) The agency that is collecting the information; and</p> <p>(ii) The agency that will hold the information; and</p> <p>(e) If the collection of the information is authorised or required by or under law,—</p> <p>(i) The particular law by or under which the collection of the information is so authorised or required; and</p> <p>(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and</p> <p>(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and</p> <p>(g) The rights of access to, and correction of, personal information provided by these principles.</p> <p>(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.</p> <p>(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.</p> <p>(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—</p> <p>(a) That non-compliance is authorised by the individual concerned; or</p> <p>(b) That non-compliance would not prejudice the interests of the individual concerned; or</p> <p>(c) That non-compliance is necessary—</p> <p>(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or</p> <p>(ii) For the enforcement of a law imposing a pecuniary penalty; or</p> <p>(iii) For the protection of the public revenue; or</p> <p>(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or</p> <p>Principle 3 subclause (4)(c)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.</p> <p>(d) That compliance would prejudice the purposes of the collection; or</p> <p>(e) That compliance is not reasonably practicable in the circumstances of the particular case; or</p> <p>(f) That the information—</p> <p>(i) Will not be used in a form in which the individual concerned is identified; or</p> <p>(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.</p>	<p>Any opt-in component of a public warning system must adhere to this principle including anywhere only certain parts of the population provide information because of their special circumstances and need for either a different message channel or assistance in certain types of emergency.</p> <p>All opt-in systems that are currently in use should have been reviewed and shown to be compliant under this section.</p>
---	--

<p>Principle 4 Manner of collection of personal information</p> <p>Personal information shall not be collected by an agency—</p> <p>(a) By unlawful means; or</p> <p>(b) By means that, in the circumstances of the case,—</p> <p>(i) Are unfair; or</p> <p>(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.</p>	<p>The number and associated address will require daily extracts from telecommunication company databases to enable moves, adds, changes and deletions.</p>
<p>Principle 5 Storage and security of personal information</p> <p>An agency that holds personal information shall ensure—</p> <p>(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—</p> <p>(i) Loss; and</p> <p>(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and</p> <p>(iii) Other misuse; and</p> <p>(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.</p>	<p>This is a condition for the agency that manages the database and any information that is sent in or out or processed.</p> <p>5 (b) will have to be complied with by any extract from the database used for sending and resending messages to numbers that are identified to be within the area of concern.</p>
<p>Principle 6 Access to personal information</p> <p>(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—</p> <p>(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and</p> <p>(b) To have access to that information.</p> <p>(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.</p> <p>(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.</p>	<p>Individual access to database information can be limited by system design to automate the process of message distribution with only those addresses not reached being viewed in an exception report.</p> <p>This Principle is less of an issue if the Privacy Commission rules that the linking of phone numbers to physical address and geospatial data does not fall within the meaning of personal information.</p>
<p>Principle 7 Correction of personal information</p> <p>(1) Where an agency holds personal information, the individual concerned shall be entitled—</p> <p>(a) To request correction of the information; and</p> <p>(b) To request that there be attached to the information a statement of the correction sought but not made.</p> <p>(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.</p> <p>(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.</p> <p>(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.</p> <p>(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.</p>	<p>Anticipating that individuals or organisations may be asked to provide information when an individual or group condition requires a special message channel or assistance, there will need to be a proactive process for ensuring that the information is kept up to date. This is to ensure that resources are not misdirected by the relocation or other changes in circumstances.</p>

<p>Principle 8 Accuracy, etc, of personal information to be checked before use</p> <p>An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.</p>	<p>As per comment to Principle 7</p>
<p>Principle 9 Agency not to keep personal information for longer than necessary</p> <p>An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.</p>	<p>Maintenance processes will need to include options to delete (not archive) information that no longer applies or where an individual or group opts not to have special needs information stored.</p> <p>In the latter instance the subscriber should be asked to sign a disclaimer absolving MCDEM of any responsibility if the conditions that led to inclusion of information still exist when it is removed. It should be widely publicised that opt-in is mandatory for those with special needs to ensure appropriate actions by emergency services.</p>
<p>Principle 10 Limits on use of personal information</p> <p>An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—</p> <ul style="list-style-type: none"> (a) That the source of the information is a publicly available publication; or (b) That the use of the information for that other purpose is authorised by the individual concerned; or (c) That non-compliance is necessary— <ul style="list-style-type: none"> (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) For the enforcement of a law imposing a pecuniary penalty; or (iii) For the protection of the public revenue; or (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or <p>Principle 10 paragraph (c)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.</p> <ul style="list-style-type: none"> (d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to— <ul style="list-style-type: none"> (i) Public health or public safety; or (ii) The life or health of the individual concerned or another individual; or (e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or (f) That the information— <ul style="list-style-type: none"> (i) Is used in a form in which the individual concerned is not identified; or (ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (g) That the use of the information is in accordance with an authority granted under section 54 of this Act. 	<p>Principle 10 (d) (ii) may grant sufficient authority for MCDEM to seek and keep information that will be useful to minimise risk to individuals, groups and emergency services.</p> <p>Refer to section 54 : “disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual”. This provides direction to define the emergency circumstances that would lead to the use of private information to facilitate a warning to all individuals and groups in the area of concern as well as provide primary intelligence for people involved in evacuation, search and rescue operations.</p> <p>The addition of personal data that has been provided by the subscriber will inform the organisations who will be engaged in assisting people to leave the area of concern. Further, availability of the personal information will allow emergency services to focus their resources.</p>

<p>Principle 11 Limits on disclosure of personal information</p> <p>An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—</p> <ul style="list-style-type: none"> (a) That the disclosure of the information 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; or (b) That the source of the information is a publicly available publication; or (c) That the disclosure is to the individual concerned; or (d) That the disclosure is authorised by the individual concerned; or (e) That non-compliance is necessary— <ul style="list-style-type: none"> (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) For the enforcement of a law imposing a pecuniary penalty; or (iii) For the protection of the public revenue; or (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or <p>Principle 11 paragraph (e)(iv) was amended, as from 3 September 1996, by section 3 Privacy Amendment Act 1996 (1996 No 142) by substituting the word “tribunal” for the word “Tribunal”.</p> <ul style="list-style-type: none"> (f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to— <ul style="list-style-type: none"> (i) Public health or public safety; or (ii) The life or health of the individual concerned or another individual; or (g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or (h) That the information— <ul style="list-style-type: none"> (i) Is to be used in a form in which the individual concerned is not identified; or (ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (iii) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act. 	<p>Any system will require access security to limit the use of information held in the database.</p>
---	--

<p>Principle 12 Unique identifiers</p> <p>(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.</p> <p>(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007 (to the extent to which those rules apply for the whole of that Act excluding the 1973, 1988, and 1990 version provisions).</p> <p>(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.</p> <p>(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.</p> <p>Section 6 principle 12(2): amended, on 1 April 2008, by section ZA 2(1) of the Income Tax Act 2007 (2007 No 97).</p> <p>Subclause (2) was amended, as from 1 April 1995, by section YB 1 of the Income Tax Amendment Act 1994 (1994 No 164) by substituting the words "section OD 7 of the Income Tax Act 1994" for the words "section 8 of the Income Tax Act 1976".</p> <p>Subclause (2) was amended, as from 1 April 2005, by section YA 2 Income Tax Act 2004 (2004 No 35) by substituting the words "Income Tax Act 2004" for the words "Income Tax Act 1994".</p>	<p>The use of unique identifiers from other databases is not required to keep the minimum information needed to ensure the safety and well being of individuals and groups.</p> <p>In the recovery and restore phases of an emergency event there may be some use for welfare agencies, among others, for information that identifies the area of impact. The location information could be used by other agencies to filter information from their own databases of client information to enable pro-active support actions. It is not perceived that the provision of summary location information would contravene any provisions of this Act.</p>
<p>54 Commissioner may authorise collection, use, or disclosure of personal information</p> <p>(1) The Commissioner may authorise an agency to collect, use, or disclose personal information, even though that collection, use, or disclosure would otherwise be in breach of principle 2 or principle 10 or principle 11, if the Commissioner is satisfied that, in the special circumstances of the case,—</p> <p>(a) The public interest in that collection or, as the case requires, that use or that disclosure outweighs, to a substantial degree, any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure; or</p> <p>(b) That collection or, as the case requires, that use or that disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure.</p> <p>(2) The Commissioner may impose in respect of any authority granted under subsection (1) of this section such conditions as the Commissioner thinks fit.</p> <p>(3) The Commissioner shall not grant an authority under subsection (1) of this section in respect of the collection, use, or disclosure of any personal information for any purpose if the individual concerned has refused to authorise the collection or, as the case requires, the use or disclosure of the information for that purpose.</p>	<p>MCDEM can assist the Commissioner by defining the rules for collection, maintenance and use of information collected for the purposes of emergency management.</p>

Appendix 5c: Mobile Premium Messaging Services Code 2008

Section	Comment
<p>4.1 Customer Consent required for all Premium Messaging Services</p> <p>All Premium Messaging Services must operate only on the basis of the Content Service Provider having received clear Customer consent from the Customer prior to the sending of any material to the Customer. For material of a nature that is charged to the Customer's mobile account, prior receipt of express consent is also required.</p>	<p>Legislation may be required that prevents any subscriber from opting-out from the public warning system</p>
<p>4.2.4 Standardisation of 'STOP' command</p> <p>Content Service Providers must adopt standard procedures to enable Customers to:</p> <ul style="list-style-type: none"> a) Unsubscribe from a Subscription Service; and b) Opt-out of marketing databases and the receipt of marketing / promotional material. <p>The following 'STOP' command and opt out procedures must be available to Customers using the Subscription Services.</p> <p>Where a Customer unsubscribes from a Subscription Services or marketing material by telephone or some means other than their mobile phone, the Content Service Provider must comply with that request within 2 Working Days following receipt for requests to unsubscribe from that Subscription Service and within 5 Working Days of receipt for requests to unsubscribe from marketing material.</p>	
<p>4.1.3 Withdrawal of Consent</p> <p>Content Service Providers must implement appropriate, legally compliant procedures to enable the Customer to notify the Content Service Provider if they no longer wish to receive any type or category of messages. These procedures must be easy to use and must minimise any inconvenience or cost to the Customer.</p> <p>Any Customer notification or request must be complied with ideally within 10 minutes of receipt, but in any event no later than 2 Working Days. With the exception of the confirmation of having unsubscribed message, no further Messages may be sent to a Customer who has notified the Message originator of their wish to opt out, unless the Customer requests or consents to the receipt of further Messages.</p>	
<p>6.1 TSP Notifications</p> <p>When a Premium Messaging Service operating on a Shortcode is to be varied, which may include any or all of the following:</p> <ul style="list-style-type: none"> a) Proposition offered on Shortcode; b) Pricepoints of Shortcode; c) Customer opt in/out procedures; d) Advertising mediums where there will be an impact to network through increased volumes; e) Customer service structures and contact details for the Content Provider; f) Change of content type or keywords; <p>the Content Service Provider must give the Telecommunications Service Provider at least 30 days written notice of the variation(s).</p>	

Appendix 5d: Telecommunications Information Privacy Code 2003

Section	Comment
<p>I, BRUCE HOULTON SLANE, Privacy Commissioner, having given notice in accordance with 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 Telecommunications Information Privacy Code 2003. Issued by me at Auckland on 2 May 2003</p> <p>Note: A code of practice issued under section 46 of the Privacy Act 1993 is deemed to be a regulation for the purposes of the Regulations (Disallowance) Act 1989 – Privacy Act, s.50.</p>	<p>This code follows the format and content of the privacy principles in the Privacy Act and will likely prove an enabler for the use of telecommunications information by MCDEM in emergency events.</p> <p>Existence of this code should shorten the time to create a code for use by MCDEM.</p>
<p>reverse search facility means a directory which is arranged, or a directory enquiry service which is operated, for the purpose of enabling an individual's name or address to be obtained by reference to a telephone number alone or an address alone, or a combination of telephone number and address</p> <p>Note: Used in Schedule 2.</p>	<p>This explains simple use of a search key that facilitates access to telephone information for the area of concern.</p>
<p>seamless means the provision of a telecommunications service in such a way that it is not evident to the subscriber that a particular service may be or has been delivered by different networks, equipment or providers</p> <p>Note: Used in rr.10(1)(h), 11(1)(l).</p>	
<p>subscriber information means personal information about a subscriber which is obtained by a telecommunications agency when that subscriber subscribes to a telecommunications service or during the term of such a contractual relationship</p> <p>Note: Used in the definition of reverse search facility"; cl. 4(1); r. 2(3); Schedule 2.</p>	
<p>4 Application of code</p> <p>(1) This code applies to information about an identifiable individual that is:</p> <p>(a) subscriber information;</p> <p>(b) traffic information;</p> <p>(c) the content of a telecommunication.</p> <p>Note: The code covers personal information collected or held by telecommunications agencies relating to individuals who subscribe to, or use, the telephone or other telecommunications services. The information privacy principles in the Privacy Act continue to apply to other personal information which is not listed here. Staff records are an example of personal information held by a telecommunications agency which is not covered by the code.</p> <p>Note: This information is collectively referred to in the code as "telecommunications information" – see cl.3.</p> <p>(2) This code applies to the following classes of agency:</p> <p>(a) a network operator;</p> <p>(b) a telecommunications service provider;</p> <p>(c) a directory publisher;</p> <p>(d) a directory enquiry agency;</p> <p>(e) an Internet service provider;</p> <p>(f) a call centre which provides call centre services on contract to another agency;</p> <p>(g) a mobile telephone retailer.</p> <p>Note: These agencies are collectively referred to as "telecommunications agencies" in the code – see cl. 3.</p>	<p>A modified code for emergency services could further limit this list to (a) subscriber information though the absence of special needs data would make the database sub-optimal.</p>

<p>Rule 10</p> <p>Limits on use of Telecommunications Information</p> <p>(1) A telecommunications agency that holds telecommunications information that was obtained in connection with one purpose must not use the information for any other purpose unless the agency believes on reasonable grounds:</p> <p>d) that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to:</p> <p>(i) public health or public safety; or</p> <p>(ii) the life or health of the individual concerned or another individual;</p> <p>(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained;</p> <p>(f) that the information:</p> <p>(i) is used in a form in which the individual concerned is not identified; or</p> <p>(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;</p> <p>(h) that the use of the information is necessary for:</p> <p>(i) the provision of a seamless telecommunications service to subscribers;</p>	<p>(h) may be a component if the identification of the message sender needs to be recognised across carriers to facilitate priority delivery</p>
<p>Rule 11</p> <p>Limits on Disclosure of Telecommunications Information</p> <p>(g) that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to:</p> <p>(i) public health or public safety; or</p> <p>(ii) the life or health of the individual concerned or another individual;</p> <p>(h) that the disclosure is necessary to enable emergency services to respond to a potential threat to the life or health of the individual concerned or another individual;</p>	<p>Modification required to enable the gathering of information prior to any event and maintained with geospatial and special needs data</p>
<p>SCHEDULE 2</p> <p>DIRECTORIES AND DIRECTORY ENQUIRY SERVICES</p> <p>1 Any disclosure made under rule 11(1)(m) must be in accordance with:</p> <p>(a) the agency's policy notified generally or to the subscriber concerned;</p> <p>Note: See clauses 6 and 7 below.</p> <p>(b) any authorisation given by the subscriber; and</p> <p>(c) clauses 2, 3, 7, 8 and 9.</p> <p>Note: See also r.2(2)(k).</p> <p>2 A network operator or Internet service provider must not make it a condition of supply of telecommunications services that subscriber information be published in a directory or be made available through a directory enquiries service.</p> <p>3 Unless the subscriber concerned explicitly authorises to the contrary, a directory publisher or directory enquiry agency must arrange a directory or operate a directory enquiry service so that:</p> <p>(a) [to search for a subscriber's telephone number:</p> <p>(i) using a directory enquiry service, an enquirer is required to provide both the approximate name and approximate address of the subscriber being sought;</p> <p>(ii) using an electronic directory, a searcher is required to provide the approximate name of the subscriber being sought;]</p> <p>Note: Clause 3(a) was substituted by Amendment No 3.</p> <p>(b) where a subscriber's name, address and telephone number is published or displayed in printed or electronic form it is ordered</p>	<p>The public warning database should not be published or available in any insecure way that would lead it to be considered a directory for the purposes of this schedule.</p> <p>A subscriber may be un-listed</p> <p>Rarely needed for emergency management by this view but the necessary reverse search facility is excluded at (d)</p> <p>Consideration of the likely Commissioner's ruling for reverse searches providing the street address</p>

<p>alphabetically by the name of the subscriber concerned;</p> <p>(c) where a subscriber's name, address and telephone number is published or displayed in a directory it is not ordered to allow searches by address only;</p> <p>(d) subscriber information is not disclosed by way of a reverse search facility;</p> <p>(e) where a subscriber has expressed a preference for his or her name to appear in the directory in a certain form, the name is not published in any other form;</p> <p>Note: For example, subscribers may prefer to be listed using initials and surname, first name and surname, or the form of name by which they are most commonly known. The directory publisher may adopt policies as to acceptable entries (e.g. in relation to length, decency or to avoid confusion) and may refuse to publish nonconforming entries or names that differ entirely from the subscriber's name. However, the agency may not publish a name in a form that differs from an expressed preference without the individual's authorisation.</p> <p>(f) where a subscriber requests that only part of his or her address is included in a directory, his or her full address is not published.</p> <p>Note: Clause 3 is modelled upon clause 13 of the Code of Practice on Telecommunications Directory Information Covering the Fair Processing of Personal Data, UK, 1998.</p> <p>4 Clauses 3(a), (b), (c) and (d) do not apply in relation to a business subscriber.</p> <p>Note: The code applies only to telecommunications information about individuals and not to information solely about corporate bodies (such as companies and incorporated societies). The business subscribers to which this clause refers are therefore individuals who are business subscribers (e.g. sole traders or some professionals).</p> <p>27</p> <p>5 Notwithstanding clauses 3(e) and (f), a telecommunications agency is not required to seek explicit authorisation from an existing subscriber as to the form in which that subscriber's name or address is to appear in a directory (including a reprinted or re-issued directory) or a directory enquiry service, but must act upon any request received.</p> <p>6 For the purposes of clause 5, an existing subscriber means a subscriber who has, [as at 1 April 2005], authorised a telecommunications agency to include his or her details in a published or compiled directory.</p> <p>Note: Clause 6 was amended by Amendment No 3.</p> <p>7 Where a telecommunications agency discloses subscriber information to a directory agency or a directory enquiry agency for the purposes of inclusion in a directory or directory enquiry service, the agency must do everything reasonably within its power to ensure that the directory publisher or directory enquiry agency will comply with the requirements of this code in relation to the publication or release of the subscriber information.</p> <p>8 Where an agency intends to seek explicit authorisation from a subscriber for a practice that would otherwise be contrary to clause 3, it must:</p> <p>(a) notify the subscriber concerned directly of the agency's policy and the available options before obtaining the authorisation;</p> <p>(b) advise the subscriber that it is not mandatory for the information to be disclosed in the directory or directory enquiry service; and</p> <p>(c) inform the subscriber that the authorisation may in the future be withdrawn and explain how this may be done.</p> <p>9 A telecommunications agency must take such steps as are, in the circumstances, reasonable to ensure that subscribers are aware of the agency's practices in relation to directories and directory enquiry services and of the options available concerning the fact and form of publication, release or withholding of subscriber details in full or in</p>	<p>without subscriber details is required.</p> <p>A key element of differentiation from usual directories is that the MCDEM database is a controlled directory compiled and used explicitly for actions required to prevent or lessen a serious and imminent threat to:</p> <p>(i) public health or public safety; or</p> <p>(ii) the life or health of the individual concerned or another individual;</p> <p>AND</p> <p>(h) that the disclosure is necessary to enable emergency services to respond to a potential threat to the life or health of the individual concerned or another individual;</p>
--	---

<p>part.</p> <p>[10. Without limiting clause 9, a telecommunications agency that publishes a directory on the Internet must:</p> <p>(a) take such steps as are, in the circumstances, reasonable to ensure that affected subscribers are aware that information about them is published in this manner and the implications for the accessibility of the information by other people (for example, any significant differences from the way in which the information may otherwise be made available in non-electronic directories);</p> <p>(b) promptly act to remove information relating to a subscriber from the Internet directory where that subscriber withdraws his or her authorisation for inclusion.]</p> <p>Note: Clause 10 was inserted by amendment No 3.</p>	
<p>SCHEDULE 3</p> <p>CALLER LINE INFORMATION PRESENTATION (CLIP)</p> <p>1 A telecommunications agency may disclose telecommunications information by means of CLIP, provided that:</p> <p>(a) subscribers are given the option to block the display of calling line identity on a per-line basis for both incoming and outgoing calls;</p> <p>(b) callers are given the means to block the display of calling line identity on a per-call basis for outbound calls; and</p> <p>(c) the agency takes reasonable steps to ensure that:</p> <p>(i) subscribers are made aware of the option to have per-line blocking; and</p> <p>(ii) users of the network are made aware of the ability to utilise per-call blocking;</p> <p>(d) simple means are available for:</p> <p>(i) obtaining per-line blocking;</p> <p>(ii) exercising per-call blocking; and</p> <p>(iii) ascertaining whether an outgoing line is blocked; and</p> <p>(e) the option to obtain per-line blocking, and the means to obtain per-call blocking and to ascertain whether an outgoing line is blocked, are made available free of charge.</p> <p>Note: Blocking prevents the identification of the calling line to the ultimate recipient of the call. Some information will necessarily be transmitted to intermediaries (i.e. between network operators) as is allowed for in rule 11(1)(l)(iii).</p> <p>2 A telecommunications agency may override any block applied pursuant to clauses</p> <p>1(a) or (b) if the call is a 111 call.</p>	<p>Clause 2 allows a telecommunications provider to override blocks. Extension of this provision would enable block overrides when the caller is '911 - Emergency please turn on radio'</p>

Appendix 5e: SMS Anti-Spam Code 2007

Section	Comment
<p>4.2 Subject to Clause 4.4, Service Providers must take reasonable steps to:</p> <p>(a) inform Customers that everybody must comply with the Act and must not otherwise not engage in practices which would result in a breach of the Act;</p> <p>(b) inform Customers of the existence of any Code of Practice applicable to Spam;</p> <p>(c) inform Customers of any relevant changes or additions to legislation applicable to Spam;</p> <p>(d) warn Customers of the consequences of breaching a Service Provider's Acceptable Use Policy in relation to the sending of Spam, including where applicable, the potential for termination/suspension of the Customer's account;</p> <p>(e) advise Customers of:</p> <p>Internet Service Providers Spam Code of Practice Page 14 of 28 Final – Version 1.00 – August 2007</p> <p>(i) methods of minimising the receipt of Spam;</p> <p>(ii) the availability of Spam Filters;</p> <p>(iii) their right to make complaints to any ISP regarding Spam that appears to come from that ISP or their customers;</p> <p>(iv) their right to make complaints to the Enforcement Agency about Spam and procedures by which such complaints can be made;</p> <p>(v) their right to make complaints to other bodies about Spam where the Content is in some way contrary to law;</p> <p>(f) inform Customers whether Electronic Messages addressed to them are subjected by the Service Provider to a Spam Filter by default, and provide a non-technical overview of the operations of that Spam Filter sufficient to assist customers in making informed choices; and</p> <p>(g) warn Customers that the use of a Spam Filter may result in legitimate emails being falsely classified as Spam (False Positives).</p>	<p>MCDEM may need to warn the public that the use of spam filters may prevent the receipt of legitimate warning messages</p>
<p>6.6 Service Providers must aim to minimise the risk of False Positives to the greatest possible extent. Service Providers should:</p> <p>6.6.1 provide contact details to which End Users or others can report False Positive incidents relating to that Service Provider</p> <p>6.6.2 consider the use of local Whitelists where whitelisted members are verified to comply with the Act</p> <p>6.6.3 avoid the use of blacklists and other Spam classification services that are known to have False Positive rates significantly higher than the industry norm</p>	<p>MCDEM may need to ensure that the source address(es) of email and SMS messages are white listed and not blacklisted.</p>

APPENDIX 6: System Descriptions

Technology	Fixed Line			Mobile Network			
Service	Voice over IVR	Fax Broadcasting	Email	SMS	SMS with Geo-Location	Cell Broadcasting (Type 1)	Cell Broadcasting (Type 2)
Description	Voice IVR messaging or autodialing is when numbers in a list are automatically dialled and a pre-recorded message is played. For example, a 36 seconds long message, delivered to 100 calls on one trunk/dialer would theoretically take one hour (3600 seconds). The number of trunks and length of the message determine the time to reach a target number of people.	Works with banks of facsimile devices. Some providers claim to be able to send 10,000s of facsimile pages per hour. The same providers may also be senders of SMS and email messaging	This service can be run in-house or using a web-based service.	Ability to prioritise SMS, by identifying channel the alert message is to be sent through and coordinating with government on the time the alert message will be sent. Ability to temporarily turn off the other channels while alert message is being sent.	Hardware can be implemented within mobile networks to capture real time information on the location of mobile devices. This means that to enable a location based public alert message to be sent to mobiles, querying the core network is no longer required therefore reducing the time and load issues around SMS. Location based service technology for mobiles is not currently being used or available within New Zealand It is a critical component of an SMS based	Type 1 Cell broadcasting is used in GSM networks to name cell sites. This allows users to see which cell site they are connected to. Identifier text appears on the top of the mobile's home screen e.g. "Wellington CBD". Character limits vary from 11 to 36 depending on the age of the mobile device. Some phones do not possess this functionality and some require it to be activated on their phones. Changes do not generate alert tones. The text can easily be	Cell Broadcasting is a point to multi-point messaging system that is an existing function of most modern digital mobile phone systems, such as GSM, UMTS and CDMA. It works through users pre-selecting on their device to have the cell broadcasting function switched on for particular channels. Network cell sites can be activated to send a broadcast message to all devices currently within its coverage area. The mobile network possesses real time information on the location of

					<p>non-opt in alerting solution. Limited commercial availability internationally. Due to commercial imperatives location based service technology is been advancing. Location based technology, termed “spatial triggering” suitable for mass public alerting is ready for implementation, however it has yet to be deployed for public alerting purposes. The person to person version of the product has been in use for some years in Australia, providing instant information to emergency services on the location of emergency calls placed on mobile calls.</p>	<p>changed by the carriers therefore could be changed to signal a CDEM emergency is in place in a particular area.</p>	<p>all devices connected to it Messages can reach millions of subscribers within in minutes. Can support up to 1350 characters (90-180 is recommended). For mass alerting the recipient receives an SMS like text message directly onto the screen of their phone, sometimes called flash messaging, which can also be set to ring and vibrate.</p>
--	--	--	--	--	--	--	---

					Some independent organisations have recognised the need for location based technology in public alerting and developed independent systems to enable it. Unified Messaging Systems (UMS) of Norway is one such organisation.		
Limits and Vulnerabilities	Capacity is limited by trunks and message length	Fax usage is largely limited to businesses		Ability to identify mobile users in an area is limited. CDMA networks cannot do this and GSM networks may take hours to run the relevant queries (depending on size of target area) and increases network loading. Message length limited to 160 characters	Not yet available in New Zealand	Limited to 11-36 characters. Available to a proportion of mobile users. May not be noticed by user of mobile device Not suitable for visually impaired	If the user does not save the message they may not be able to retrieve it again Limited to devices that support this functionality and to those subscribed to the appropriate channels. The ITU is currently performing work to ensure international standardisation of these channel addresses. New

							Zealand deployment would need to ensure internationally consistent standards are developed and implemented across the national carriers. The elderly may be particularly less inclined to do this due to their lack of familiarity with device technology. As a device function, users can not be automatically connected to this service at a network layer.
Strengths	Available in NZ nationally now Ability to distinguish between live response and answer machines. Less likely to be ignored than mobile technologies. Message length	Available in NZ nationally now	Available in NZ nationally now Message length not limited (?)	Available in NZ nationally now Sensitive to power loss. Wide spread prolonged power outage i.e. over 24-48 hours has potential to severely degrade coverage. Potential for delay between sending	Overcomes loading and delay issues in sending SMS to mobile devices in target areas	Available in NZ nationally now Messages can be quickly generated for target areas with no loading issues	Could be deployed in New Zealand now Messages do not present load congestion issues and is purported to work in a fully congested network Different channels can be set to

	not limited			and receiving due to ability to turn off, and ignore incoming messages. Aged do not like text messages. Public alerting opt in solutions require alternate means to opt in. Mobile device text alerts may not wake sleeping target receivers.			communicate different emergency information ie.g. different languages, deliver different messages to first responders
Additional Features	Autodialing may be accompanied by voice to text or text to voice conversion to suit the requirements of the receiver e.g. the blind or deaf			Can cater for non-English speakers, however messages would likely be pre-programmed to ensure speed of message delivery. Not designed for vision impaired, however text to voice conversion products are available to end users. If users were required to opt-in and an integrated system was selected users could elect			Geo-scalable from a single cell site coverage area to a whole country. Accommodates disability related technology

				to have a voice message sent to their mobile as an alternative			
Recommendation	Most useful for early warning of small target areas	Most useful for business areas during work hours		Most useful in initial stages of an event when a network is not congested and target audience is not likely to be sleeping. However if paired with congestion control mechanisms it may be suitable in some events.	When available it will be suitable for sending messages to targeted areas.	Useful alerting supplement for rapid deployment of very short messages.	Cell broadcasting is an attractive public alerting solution given its delivery speed and ability to continue working in a congested network environment.
Examples / References				Mobile Network	http://www.ericsson.com/technology/positioning_methods/spatial_triggers.shtml		In Korea cell broadcasting is used for distribution of supermarket discount vouchers
				SMS			

APPENDIX 7: Mobile Telecommunication Market

New Zealand currently has two primary providers of mobile services, Telecom New Zealand and Vodafone NZ. Mobile market penetration is very high in New Zealand at over 80%. Currently the providers are relatively evenly split in terms of market share with Vodafone having 53% (2.4 million customers) and Telecom having 47% (2.2 million) as of first quarter results in 2008. Telstraclear signed an agreement with Telecom in August 2007 launching its own mobile service in November 2007, providing a unique range of mobile services, bundles and prices via the Telecom network initially with business customers. Consumer customer services were launched in August 2008.

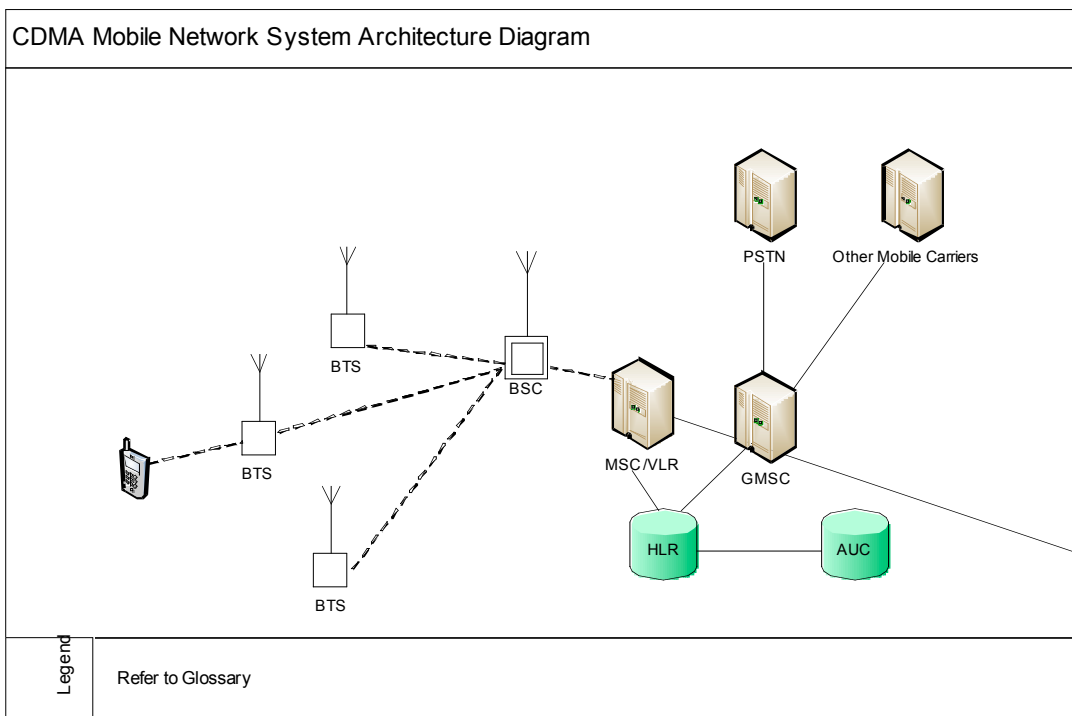
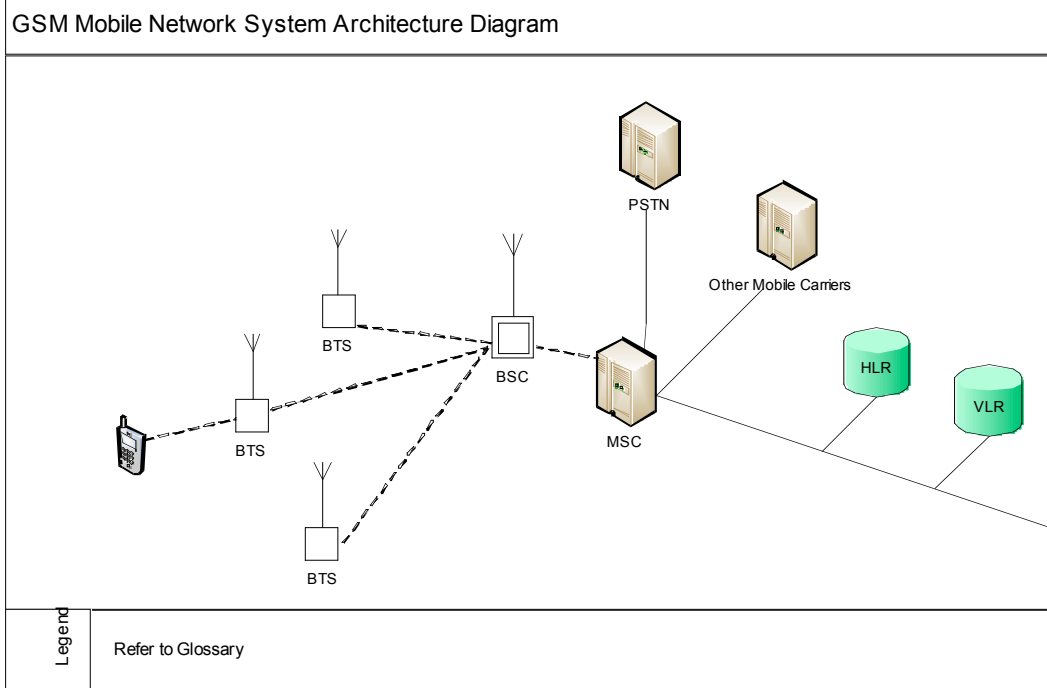
Recent legislation changes have required the incumbent mobile providers to provide both roaming access to new network providers whilst they build their own network and co-location of cell sites with the new providers. NZ Communications is expected to be the first new mobile provider with an initial proposed launch date of end of 2008, which has recently been moved to late 2009¹.

Vodafone NZ currently runs a GSM based mobile network, whereas Telecom uses a CDMA network. Vodafone is in the process of rolling out W-CDMA technology through its 3G sites. Telecom is also going through a technical deployment of a new mobile network based on UMTS/W-CDMA technology with a GSM edge, 2G coverage will be fully implemented at the proposed launch date, end of 2008 with 3G being rolled out to all major cities over the next two to three years.

¹ Drinnan, J. 2008. Expanded Mobile hits snag. *NZ Herald August 19, 2008*.

APPENDIX 8: Mobile Network Configuration Diagrams

The diagrams below show a high level representation of the GSM and CDMA network configurations.



APPENDIX 9: Global Positioning Systems and Public Alerting

"A Satellite-Based Communication Channel for the Reliable Distribution of Early Warning Messages"² discusses the use of Satellite-Based Augmentation Systems (SBAS) to communicate alerts using existing augmentation infrastructure within the Global Positioning System (GPS). SBAS systems are active over Europe (European Geostationary Navigation Overlay Service - EGNOS), North America (Wide Area Augmentation System - WAAS), and Japan (Multi-functional Satellite Augmentation System - MSAS).

Design principles behind SBAS are conducive to alerting due to the following characteristics as outlined by Plag et al:

- Institutionally controlled systems
- Secure
- Operated for safety of life applications
- Guarantee adequate message broadcast
- Integrity of messages
- Confirmation of transmission

None of the current or planned SBAS are or will be publicly available over New Zealand. OmniStar provides a commercial service, however only expensive survey-provision GPS equipment appears to support this subscription-based service and New Zealand coverage is not comprehensive.

It would be prohibitively expensive for New Zealand to invest in a system on our own due to the cost of launching a geosynchronous satellite that is required to broadcast the SBAS signal; however it may be possible to implement on a regional basis - such as the South Pacific or Oceania. The benefits of a SBAS to the region would include more than just alerting, as it would provide improved accuracy for navigation and other economic benefits.

² Mathur, A. R., Ventura-Traveset, J., Montefusco, C., Toran, F., Plag, H.-P., Ruiz, L., Stojkovic, I., & Levy, J. C., 2006. Provision of emergency communication messages through SBAS: the ESA ALIVE concept, in ION GNSS 2005 Proceedings, Long Beach, California, 2969-2975, Institute of Navigation, USA (pdf). From <http://geodesy.unr.edu/hanspeterplag/publications/> Accessed 20081003

APPENDIX 10: Interviewees

Information was received from the following people as part of the project:

**A3M AG - Tsunami Institute,
Deutschland (www.tsunami-alarm-system.com)**

Marcel Brandt (Head of Marketing)

CEASA UK (www.ceasa-int.org)

Mark Wood (Hon. Sec.)

**Cellcast Technologies US
(www.cellcastcorp.com)**

Paul Klein (C.E.O)

Kevin Preston (C.I.O.)

Ericsson Australia

Patrick Quin (Account Manager)

FESA (www.fesa.wa.gov.au)

Stephen Johnston (Manager Operational Development)

Gen-i

Judson Croft

Kordia

Alan Mordecai (Manager Infrastructure and Property Group)

Rocom NZ

Richard Guy (Director)

John Nowak

Telecom NZ

Brian Potter (Risk Manager)

Brigitte Theuma (Business Continuity Manager)

Dean Schmidt (Head of Government Relations and Community Relations)

Andrew Bowater (Adviser, Government and Community Relations)

Presan da Silva (Enterprise Architect)

Grant Cromby (Telecom Mobile (W-CDMA))

Gavin Dudley (Sales Manager)

Malcolm Shore (Technology Strategist)

Telstra

Mark Stevens (Senior Sales Specialist)

TelstraClear

Dilshan Perrera (Principal Systems Architect)

Robert Visscher (Account Manager)

UMS Norway

Morten Gustavsen (Managing Director)

Kjell Heen

Vodafone Australia

Claudine Everitt (BCM Manager)

Vodafone Italy

Marilena Tardito (ICT Security & Privacy)

Vodafone NZ

George Bromell (Senior Engineer, Value Added Services)

Peter Carr (BCM Manager)

Claire Green (Sales Operations Manager)

Mandos Mitchinson (Operations Manager

– Fixed Line and Broadband)

Callum O'Neill (Core Services)

Alan Roberts (Service Enablers)

Murray Smith (Roaming Specialist)

Brandon Wong

Vector Communications

Kevin Oswin

Vodafone UK

Amanda Chandler (Data Protection and Business Continuity Manager)