

The Value of Government Mandated Location-Based Services in Emergencies in Australia

Anas Aloudat, Katina Michael, Roba Abbas

School of Information Systems and Technology, University of Wollongong, Australia

Keywords: emergency warning, national security, standards, public policy, emergency declaration, emergency response, location-based services, socio-ethics, regulation, emergency alert

ABSTRACT

The adoption of mobile technologies for emergency management has the capacity to save lives. In Australia in February 2009, the Victorian Bushfires claimed 173 lives, the worst peace-time disaster in the nation's history. The Australian government responded swiftly to the tragedy by going to tender for mobile applications that could be used during emergencies, such as mobile alerts and location services. These applications, which are becoming increasingly accurate with the evolution of positioning techniques, have the ability to deliver personalized information direct to the citizen during crises, complementing traditional broadcasting mediums like television and radio. Indeed governments have a responsibility to their citizens to safeguard them against both natural and human-made hazards and today national security has grown to encapsulate such societal and economic securitization. However, some citizens and lobby groups have emphasized that such breakthrough technologies need to be deployed with caution as they are fraught with ethical considerations, including the potential for breaches in privacy, security and trust. The other problem is that real world implementations of national emergency alerts have not always worked reliably and their value has come into question as a result. This paper provides a big picture view of the value of government-mandated location-based services during emergencies, and the challenges ensuing from their use.

INTRODUCTION

The aim of this article is to present a case study on how modern technologies, namely mobile applications, are changing the landscape of emergency management in Australia. The article begins by providing a general overview of emergency management and location-based services and then specifically places the reader in an Australian context by describing recent trends in emergency response, especially post the Victorian Bushfires of February 2009. The introduction of new warning and alerting methods and techniques will be a critical element in securing the nation against diverse natural hazards such as bushfires and floods. In today's modern age of technological innovation, it is difficult to comprehend how 173 persons perished and 414 persons were injured during the Black Saturday crisis, partly as a result of accessibility to timely and relevant information on how to respond to the emergency.

The recently deployed national emergency warning system (NEWS), as well as future "location-enabled" components, will be discussed before socio-ethical considerations are

explored. It is anticipated that NEWS will force amendments to the *Telecommunications Act 1997*; an issue that was first tabled by the Australian Federal Government. With the pending introduction of such advanced technologies, it was also deemed that the regulations governing the use of the Integrated Public Number Database (IPND) also be reviewed. The IPND grants some government agencies access to Australia-wide consumer telecommunications details during emergencies and is maintained by one commercial mobile operator but may need to be accessed by more than one commercial entity during an emergency.

There are thus a number of socio-ethical considerations which need to be taken into account when reviewing both regulation and legislation in this domain. Despite the potential for breaches in privacy, mobile technologies and specifically location-based services offer a state-of-the art solution to the age old problem of personalized information dissemination based on context. Where a new technology can act as a life-sustaining tool, privacy issues are generally considered less important and wholly overshadowed by issues related to trust. Very few people would opt not to disclose their real-time physical location in the name of privacy, if it meant that they could survive a natural disaster. What is of greater concern to the success of an emergency service offering however, is that users can trust the technology, can trust the supplier of the service, and can trust that the accuracy, reliability and timeliness of the communicated message during a crisis. The findings of the study demonstrate that location-based services are a plausible solution to emergency management problems in Australia and that the benefits to citizens of using such innovations during natural disasters are clear. This does not mean however that government mandated services to citizens are not without their specific risks. Location based mobile alerts for emergencies, for example, are still experiencing significant teething problems in implementation which has brought their value into question. Citizens would rather have no information at all, rather than delayed or inaccurate information about an emergency which is purported to be near their real-time location.

EMERGENCY MANAGEMENT IN AUSTRALIA

Defining Natural and Human-Made Hazards

Managing emergencies with regard to their socially-constructed context is one of the reasons that has led Australia to adopt the all-hazards approach in responding to risks associated with physical phenomena (Templeman & Bergin, 2008). A hazard is any source of potential harm or a situation with a potential to cause loss (Emergency Management Australia, 2004b). Emergency Management Australia (EMA) defines many types of hazards, which are broadly classified. Most of the known hazards are considered natural because they have their origins in the surrounding natural environment. Examples include bushfires, floods, cyclones, tsunamis, landslides, windstorms and earthquakes. Several other hazards are identified as technological, which are the result of failures in human-made systems and services, or are the outcome of human actions. For example, these include urban structure fires, explosions, and transportation incidents. Some hazards are classified as chemical, biological or radiological due to their specific origin. Some examples of these are toxic material releases, human epidemics and pandemics, exotic animal diseases, and insect and vermin plagues. Remaining hazards can be classified as social in origin, which include civil unrests and acts of violence such as riots, sieges, shooting massacres, hijackings, sabotage and terrorism (Emergency Management Australia, 2008). Table 1 summarizes the different types of hazards.

Table 1. Hazard Types

Hazard Classification	Types
Natural hazard	Bushfires, Cyclones, Earthquakes, Floods, Hurricanes, Land gales, Landslides, Mudslides, Storm surges, Tidal waves, Torrential rain, Tsunamis

Technological hazards	Blackouts or main power failures, Explosions, Mining or industry incidents, Pollution, Smog, Transportation incidents, Urban structure fires
Chemical, biological and radiological hazards	Chemical emissions, Epidemics / Pandemics, Exotic animal diseases, Insect or vermin plagues, Toxic spills
Social in origin hazards	Civil unrests, Hijackings, Riots, Sabotage, Shooting Massacres, Sieges, Terrorism

Throughout history, communities have battled hazards and responded to emergencies with the commensurate technology available to them. Organized attempts to counter emergencies, however, did not occur until much later in modern times (Haddow, Bullock, & Coppola, 2006). These attempts have evolved from simple precautions and scattered actions into systematized and sophisticated policies, programs and applications that include preparedness, response, mitigation, recovery and protection strategies (Canton, 2007). Modern emergency management (EM) could be defined as the discipline dealing with risk and risk avoidance and primarily concerned with developing and improving arrangements and programs that contribute to the goal of a safer, more sustainable community (Haddow, Bullock, & Coppola, 2006).

Emergencies in Australia

The Commonwealth of Australia covers a land mass of approximately 7,692 million square kilometers with a population of about 22 million. Around 85 percent of the population live in cities within 50 kilometers of the coast, where much of the country's commercial and industrial activity takes place (Australia.gov.au Website, 2010). Australia is divided into six States and two Territories. Each State or Territory has its own government, legislature and constitution. The legislature of Australia comprises a bicameral federal parliament, with a Prime Minister and Cabinet (PM&C).

As a physically large country with a diverse climate and geographic landscape, Australia experiences many types of hazards on a regular basis (Boughton, 1998). In addition, communities across Australia continue to settle into hazard-prone areas, particularly in coastal and river valley regions, exposing themselves to risks from a variety of sources including cyclones, floods and bushfires (The Victorian Bushfires Royal Commission, 2009). Even in regional areas, and as a result of inadequate risk assessments and mitigation actions, transport infrastructure, such as road and rail links, are usually flooded annually, which cause disruption to the carriage of commodities for communities and business, and the supply of materials for industry (The Australian Government: Department of Transport and Regional Services, 2004).

Reliable information on the frequency of emergencies and disasters in Australia extends only from 1967; nonetheless, the number of events has shown an upward trend in frequency over the last 20 years (The Victorian Bushfires Royal Commission, 2009). The same trend is noted worldwide both in the developed and developing countries, caused by several factors including an increase in human activities in hazard-prone areas, military conflicts and climate change (Coyle & Meier, 2009; United Nations News Centre, 2010). Despite that the frequency of emergencies and the numbers of people who live or work in risk-prone areas have increased in Australia, deaths per 100,000 population have continued to fall due to better emergency management policies, arrangements and applications (The Australian Government: Department of Transport and Regional Services, 2004).

Emergency Management Arrangements in Australia

Under Australia's constitutional arrangements, the country takes a Federal approach to emergency management in which the local, state and territory governments have responsibility within their own jurisdiction and have the laws, funding mechanisms and

organizational arrangements in place to deal with emergencies. Each sphere of government has a different set of roles and responsibilities for emergency planning, preparedness and mitigation in relation to land, property and the environment, assets and infrastructures, agencies and programmes (Emergency Management Australia, 2009a).

Given that individual States and Territories are highly autonomous, the approach to emergency planning and alerting in Australia is not standardized (The Australian Government: Department of Transport and Regional Services, 2004). Nonetheless, there are similarities in approach that have emerged between states. For example, should a state of emergency be declared, a state-level emergency/disaster response and coordination committee/executive acts as the interface responsible for coordinating the state resources, seeking Commonwealth support if needed, and providing up-to-date reports to the media (Victorian State Parliamentary Offices, 2003). When activated, the committee is mainly responsible for:

1. Information collection, analysis and dissemination of intelligence to emergency response agencies;
2. Coordination of the provision of resources required by divisional emergency response coordinators;
3. Allocation of resources on a priority basis;
4. Requesting Commonwealth physical resources;
5. Briefing the Coordinator in Chief; and
6. Dissemination of information to the media and general public (The Victorian Bushfires Royal Commission, 2009).

The level of emergency response coordination depends on the scope of the emergency. In the first instance, the response to an emergency takes place at the municipal level. If the emergency calls for resources beyond those available at the municipal level, the emergency response coordination is stepped up to the divisional level. An emergency that extends beyond the division will be progressed to the State level (The Victorian Bushfires Royal Commission, 2009).

Although the prime responsibility for the protection of life, property and the environment rests with the states and territories, the Commonwealth Government is strongly committed to supporting local and state governments in developing their capacity for dealing with emergencies and disasters, providing physical assistance and mobilizing resources to States or Territories when they cannot reasonably cope during large-scale events (Emergency Management Australia, 2009a). On the national level, the basis for managing major emergencies and combating disasters is a partnership between the Federal, State and Territory, Local Governments, the community, and the private sector. Accordingly, this national framework for emergency management requires a high level of collaboration and coordination across all spheres of government, and with other non-government stakeholders as well (Emergency Management Australia, 2009a).

Emergency Management Committees and Organizations in Australia

Emergency and disaster management committees and organizations exist at National and State/Territory levels in Australia with specific responsibilities for local governments within their jurisdiction. The main emergency management bodies in Australia include:

1. The Commonwealth Counter Disaster Task Force: A senior interdepartmental committee, chaired by the Department of the Prime Minister and Cabinet. It is the peak Commonwealth body with emergency management responsibilities composed of representatives of Commonwealth Government departments and agencies with a significant role to play in the provision of disaster relief or rehabilitation assistance. On the advice of the Director General of the Emergency Management Australia (EMA) agency, the Chair may activate the committee during the response and

- recovery phase of a disaster in support of EMA's activities (Emergency Management Australia, 2004a).
2. The Australian Emergency Management Committee: Australia's principal consultative emergency management forum. It is chaired by the Director General of EMA, and comprises chairpersons and executive officers of State and Territory emergency management committees. The Committee meets bi-annually to provide advice and direction on the coordination and advancement of Commonwealth and State interests related to emergency management issues. As required, it establishes working parties to examine particular issues (Emergency Management Australia, 2004a).
 3. The State and Territory Emergency/Disaster Management Organizations: Each State and Territory has established a committee of senior members of appropriate departments and agencies to consider emergency management matters. The names and functions of these organizations differ from State to State, but they are responsible for ensuring that proper plans and arrangements are made at State or Territory and local government level, to alert the public to and deal with emergencies and disasters (Emergency Management Australia, 1996).
 4. Emergency Management Australia (EMA): The Federal agency through which the Attorney-General exercises the responsibility of providing national leadership in the development of emergency management measures to reduce the impact of emergencies on the Australian community (Emergency Management Australia, 2004b). EMA is mainly responsible for shaping and advancing emergency management strategies and policies throughout Australia, advocating emergency management education, and assisting state and territory local emergency management agencies. EMA also plays a key role in coordinating interstate and international assistance at times of major emergencies and disasters (Emergency Management Australia, 2004b). EMA has an established collaborative relationship with other Commonwealth agencies such as the Department of Finance and Administration, Geoscience Australia and the Bureau of Meteorology. In doing so, EMA seeks to encourage an all hazards, all agencies approach to the prevention or mitigation of emergencies, preparedness for their impact, response to that impact and recovery from the consequences (Emergency Management Australia, 2009b).
 5. Other committees and organizations exist at the State level in Australia. The names and functions of these organizations and committees differ from State to State but there are similar patterns that have been developed between them in regard to their roles and functions that include the identification of various threats and hazards, the coordination of volunteers and community resources during significant emergency events, hazard management guidelines, declaration of state of emergency, emergency management training and education, and the arranging of warnings in emergencies to the public (The Australian Government: Department of Transport and Regional Services, 2004).

An All-Hazards Approach to National security in Australia

The Changing Face of Emergency Management

Until recently emergencies were quantified in terms of the loss of life, extent of damage, or based on an event's physical attributes (Emergency Management Australia, 2004b).

Emergencies have been traditionally associated to the notion of a "disaster" when the number of casualties and the allocated resources to a given event have been high (Canton, 2007).

More contemporary viewpoints, especially from the social sciences have begun to question the validity of traditional classification schemes that have long defined emergencies and disasters or distinguished them according to their origin or scale. Social studies started to perceive these events as social constructions, defined by the nature and the volume of their impact on social systems (Perry, 2007; Quarantelli, 1986; Rosenthal, 1998).

The focus in understanding emergencies has now shifted toward the actual situation created by such phenomena, rather than simply considering the physical attributes that caused them (Emergency Management Australia, 2004b). This shift has come as a result of a growing realization that although there are many different types of emergency events, whether natural- or human-caused, they all have comparable capacity to bring social, economic, environmental and political consequences on the communities they impact (Buzan, Wver, & Wilde, 1998; Rosenthal, 1998). Thus an emergency impacts the organization of human communities and can be thought of only within a larger framework involving the society as a whole (Gilbert, 1998). It is what has caused a redefinition of national security to incorporate large-scale emergencies, and not just things to do with the military. How a government responds to a large scale emergency today has as much to do with national security as traditional security-centric actions like border control. Yet while the government aims to protect the well-being of its citizenry through blanket coverage technologies such as location-based services, they still need to maintain an individual-level of consent. For example, the government's adoption of sophisticated unmanned aerial vehicles (UAVs) to keep out illegal immigrants is very different to the government communicating with citizens via their personal mobile phones, especially when an entity's real-time location can be determined.

The Comprehensive and Integrated Approaches

Australia has adopted both a comprehensive and integrated all-hazards approach to the development of its arrangements and programs. The approach can be summarized as follows. Under the comprehensive approach there is a general acknowledgment that a potential threat could originate from various types of hazards which have a comparable capacity to impact severely on communities and infrastructure. The all hazards approach to emergency management involves a recognition that most emergency event types cause similar problems and that many of the measures required to deal with them are generic (The Victorian Bushfires Royal Commission, 2009). Australia's comprehensive approach to emergency management identifies four strategies that contribute to the reduction or elimination of hazards, and an increase in community and environmental resilience. EMA (2004b) defines these strategies as follows:

1. Prevention/mitigation: Seek to eliminate or reduce the impact of hazards and/or to increase the resilience of the community subject to the impact of those hazards.
2. Preparedness: Concerned with establishing arrangements and plans and with providing education and information so as to prepare the community to deal with emergencies and disasters as they may arise.
3. Response: Covers the methods that are used to properly activate the preparedness arrangements and plans so as to deal with emergencies and disasters if and when they occur.
4. Recovery: Defines the set of arrangements practiced to assist a community affected by an emergency or disaster in reconstruction of the physical infrastructure and restoration of emotional, social, economic and physical well-being.

These emergency management strategies, although tightly related, could be developed independently of each other (Haddow, Bullock, & Coppola, 2006). Nonetheless, under the comprehensive approach to emergency management there is an emphasis that all of the activities, under these strategies, should effectively function as one seamless emergency management framework (Emergency Management Australia, 2004b; Haddow, Bullock, & Coppola, 2006).

The integrated approach emphasizes the need to coordinate different emergency management programs and strategies with the support of other government agencies, and with the community and the private sector (Emergency Management Australia, 2004b). For the comprehensive approach to emergency management to be workable there should be effective arrangements for the coordination of the activities of governments and of the large number of organizations that need to be involved in emergency management activities. These

arrangements need to be set within a legislative and public policy framework (Emergency Management Australia, 2004b). It therefore follows that technological solutions deployed to protect citizens also need to be set within a legislative and public policy framework. The problem however with “emergencies”, whether they are natural or human-made is that they strike with little warning, if any, and therefore the deployment of specific technologies during a given emergency (e.g. with the requirement for access of citizenry personal data) undergoes limited discussion.

THE EMERGENCE OF LOCATION-BASED SERVICES SOLUTIONS

What are Location-based services?

Location-based services (LBS) are also known as location-dependent services, location-related services, location-enabled services, location-sensitive services and location services. See for example the definitions given by Hjelm (2002), Jensen (2002), Holma et al. (2004), Lopez (2004), Spiekermann (2004), Bernardos et al. (2007) and Uhlirz (2007). Küpper (2005) has previously noted this and argued that one possible reason for terms being used interchangeably is that the character and appearance of LBS have been specified and implemented by different communities and industries, especially in the telecommunications sector and the ubiquitous computing area for a variety of applications. In the context of LBS, *location* always refers to a spatial geographical location that is associated with a physical point or region relative to the surface of the Earth (Dawson, Winterbottom, & Thomson, 2007). Accordingly, LBS are classified as a subset of a larger set called context-aware services, which are electronic services that automatically adapt their behavior (e.g. filtering or presenting information) to one or more parameters (time, location, identity or activity) so as to reflect the context (personal, technical, spatial, social, or physical) of a target (person, animal or object) (Küpper, 2005).

LBS as a concept denotes applications that utilize the available geographic location information of a target device, being fixed, handheld, wearable or implantable, in order to add value to the provided service (Perusco & Michael, 2007; The 3rd Generation Partnership Project, 2009). Astroth (2003) defines a LBS as “any application that offers information, communication, or a transaction that satisfies the specific needs of a user in a particular place.” Harvey (2008) simply defined LBS as “technologies that add geographical functions to other technologies.” Gruber and Winter (2002) argued that a LBS is “any value-added service that takes into account a mobile agent’s actual location.” Shiode et al. (2002) delineate LBS as “services that provide geographically-orientated data and information services to users across mobile telecommunication networks.”

Samsioe and Samsioe (2002) assert however that an electronic service that has location capabilities, should be able to fulfill the following three separate activities to be accurately defined as a LBS:

1. Estimate the location of the device;
2. Produce a service based on the estimated location; and
3. Deliver the location-enhanced service to that device.

Based on Samsioe and Samsioe (2002), this strict definition excludes several services that employ location technologies in mobile telecommunications networks such as the cell broadcasting service, since these services cannot change their content when the physical location of a mobile handset changes. However, in the emergency management context, it should be understood that any service that provides information pertinent to the current location of the active mobile handset at a specific period of time can be viewed as a location-based service, regardless of the underlying delivery technology used to convey its information. Although this interpretation may extend to other types of services as well, it is nonetheless, an understanding that harmonizes several different forms of LBS such as those depicted by Holma et al. (2004), Grothe et al. (2005), Guan et al. (2007), Oh and Haas (2007), Stojanović et al. (2007) and Aitenbichler (2008).

The text-based message is the most realized form of LBS, but there are several other possible forms where the service could be received as a bitmap image, voice message, multimedia message (with rich content such as animated image formats), interactive maps or video. However, the final form of the delivered LBS depends on several factors that include existing and dedicated network resources, underlying technologies and protocols, market trends and handset capabilities/ limitations (Spiekermann, 2004).

Operational and Non-Operational Stakeholders

Effective deployment of location-based services requires the coordinated effort of multiple stakeholders in the services value chain, each of which provide specific components of the total solution (Astroth, 2003). A stakeholder represents an autonomous entity like a person, a company or an organization, each maintaining or performing one or several roles that characterize either the interests or functions it fulfils from a technical perspective, or the impact it exercises on LBS from an economic or regulatory position (Küpper, 2005).

Roles of LBS stakeholders can be classified as operational and non-operational. The operational roles define the players that cooperate during the operation of the service, which requires each stakeholder to maintain technical infrastructure, ranging from users' mobile handsets to service providers' farm servers to carrier's telecommunications networks, so as to facilitate the request and the provision of sub-services during LBS execution (Küpper, 2005). During an LBS operation, the interaction between these actors takes place through reference points that are defined by a set of protocols and connectivity services offered by various networks, and often determined by Service Level Agreements (SLAs). SLAs are agreed upon and adopted between the participating parties, prior to the provisioning of the services, for fixing quality of service and accounting conditions (Küpper, 2005). With so many stakeholders involved in a single LBS offering, upkeeping locational privacy is not easy. This is where industry level guidelines, contractual agreements between stakeholders, or even company level codes of conduct can play a pivotal role in protecting citizen rights.

A non-operational stakeholder is the one that does not directly engage in the technical operation of LBS but has an indirect impact on the services, either by dictating economic or regulatory circumstances of LBS operation or through the influence it exercises on the adoption of technical service standards (Küpper, 2005). An example from the Australian context could be Australian Communications and Media Authority (ACMA) which exercises a direct influence in regulating (by law) the utilization of location data to protect the privacy of individuals and for other purposes such as lawful interception (The Australian Communications and Media Authority, 2004).

Evolution of Global Positioning Techniques for Location-Based Services

The first location system in use was the satellite-based Global Positioning System (GPS) created, funded and controlled by the U.S. Department of Defense. The system was built and conceived primarily to serve military purposes but since the late 1990s the system was upgraded with new civilian signals making it freely available to the public and commercial use (Kaplan & Hegarty, 2006). The result of this free availability of satellite positioning capabilities led to a real revolution in a wide range of applications that include air, sea and land traffic control, navigation solutions, freight management, and emergency services (Spiekermann, 2004). Other comparable GNSSs are currently also in use or scheduled to operate in the very near future. One such system is the European Union satellite system of Galileo, a GNSS with meter-range accuracies appropriate for applications such as safety and navigation (European Space Agency, 2011).

According to the European Commission (2011), advantages can particularly be attained through the combination of Galileo and GPS capabilities. The Galileo project is presently in

the operational stages of development, given the launch of the initial two satellites in 2011 and with two more scheduled for 2012 (European Space Agency, 2011). The development and operation of Galileo is expected to provide enhancements to existing positioning techniques, providing higher levels of accuracy, connectivity and real-time location data, which will have implications for applications areas such as emergency management.

Location-Based Emergency Services in Mobile Networks

Emergency services represent one of the most obvious application areas where the deployment of location technology makes sense (Küpper, 2005). Still, location-based emergency services are in their infancy in several countries around the world including Australia (Küpper, 2005). One reason for this, beyond the socio-ethical issues are technical problems, including location determination mechanisms and accuracy standards, and also issues related to identifying different requirements for emergency systems which have yet to be fully resolved (The European Telecommunications Standards Institute, 2010; Togt, Beinat, Zlatanova, & Scholten, 2005)

In general, there are two types of location-based emergency service applications in mobile telecommunications networks (The European Telecommunications Standards Institute, 2006a). The first is initiated by a person in the form of a phone call or a distress Short Message Service (SMS) in a life-threatening or time-critical situation. The second type is initiated usually by the government in collaboration with telecommunications carriers, in which safety alerts and early warning messages are disseminated (pushed) to all active mobile handsets located in designated threatened area(s) before, during or after a large-scale event. The fundamental idea behind the first type of location-based emergency service application is for an emergency service organization (ESO) (i.e. police force, fire brigade or ambulance service) to reach the caller (or the message sender) with some precision, based on the location information provided by the caller's mobile service provider. In many cases the person will be unable to communicate his or her current location or simply does not know it, so the ESO relies on handset data (Küpper, 2005). The premise behind the second type of emergency service application is to utilize the mobile handset as an additional information channel that is capable of reaching people wherever they are but within the threatened area.

EMERGENCY WARNING AND ALERTING METHODS IN AUSTRALIA

Traditional Warning and Alert Systems

Under emergency management arrangements in Australia, one of the main responsibilities of the government is to communicate and disseminate warnings and safety information to the general public in case of a large-scale emergency (The Australian Government: Department of Transport and Regional Services, 2004). In principle, any means of ensuring that a warning is quickly disseminated to those actually or potentially affected should be used. However, conventional broadcasting systems consisting primarily of local community radio stations and television networks are still the main channels that are currently used for disseminating alerts and warnings to the Australian public (Betts, 2003).

Australians also rely on several other sources of information, including relevant government websites and hotlines, to stay updated with the latest news about events as they unfold. In addition, traditional warning methods are used across the country including banners, door-to-door knocking and signage. Australia also still relies on what are known as triggers, such as the standard emergency warning signal (SEWS) and associated sirens, which are merely techniques prompting the audience to listen carefully for a warning and/or to search for more information (The Victorian Bushfires Royal Commission, 2009).

Modern Warning and Alert Systems: The Short Message Service and Beyond

Other means and methods such as emails, landline and mobile phone calls, and short message service (SMS) have also been considered or used. For example, Telstra (the incumbent

telecommunications operator) partnered with the state of Victoria in 2005, to trial the Community Information Warning System (CIWS) that was able to simultaneously telephone every household in a designated area. More than 660 calls were made, on an opt-in basis, to the residents of one specific area who had volunteered to participate in the trial (The Minister for Police and Emergency Services, 2005).

In 2007, SMS and email alerts were considered by the Victorian State Government for the purpose of geographically targeting people in specified areas with information about terror attacks or natural disasters (Dunn & Collier, 2007). In the same year, the New South Wales Premier proposed a warning system for metropolitan Sydney whereby residents could opt-in to real time Government SMS and email air pollution health alerts. The proposal came in response to key recommendations from a Parliamentary air quality inquiry in 2006, which warned that 1600 people were dying every year from air pollution related illness in New South Wales. This project was under the Department of Environment authority (Benson, 2007). The New South Wales Government also proposed an electronic warning system that, in principle, should have allowed ESOs, such as Police, Fire and Ambulance services, to send SMS alerts to all mobile handsets in terrorism or emergency target zones across the State. The design concept identified the system's need to be operable across all telecommunications carrier networks operating in Australia, and was to provide evacuation information, safety advice and alternate routes to avoid the emergency area (The Australian, 2007).

A similar system is now active in Sydney, New South Wales. The SydneyAlert system is a free, opt-in service that is meant to alert the general public in the event of an emergency in the Sydney and North Sydney Central Business Districts (CBDs). The system provides building managers, emergency wardens and security staff with safety information and instructions to help them manage and assist occupants, staff and others in their buildings during a serious incident. The system uses existing commercial communications networks to disseminate warnings, specifically SMS and e-mail. The State Emergency Operations Centre Controller, a senior NSW Police Officer, is the authority that determines if the system should be activated. This officer also determines who on the subscription list is contacted and what message is sent. The message is sent to the contact details supplied by those who have subscribed to SydneyAlert. The message is simple, giving clear guidance on what needs to be done. Example messages include: "Evacuate to a safety site", "Stay indoors and close windows", or "all clear message and situation is back to normal" (New South Wales Government, 2007).

Despite the SMS technology being available before the Victorian Bushfires, it was not until after the fires in 2009 that it was used to alert Victorians about severe weather conditions and other threatening bushfires (Dobbin, 2009; Ife, 2009). With fire risk and high wind predicted across the state, Telstra, Optus and 3 Hutchison- the three main mobile service providers in Australia- sent SMSs on the third of March 2009, on behalf of the Victorian Government and Victorian Police to more than 3 million mobile subscribers, advising recipients to listen to the Australian Broadcasting Corporation (ABC) radio for emergency updates (Dobbin, 2009; Ife, 2009). The messages were sent using commercial services (i.e. as part of a community service obligation), and not part of any State or National emergency warning system (ABC News, 2009). Some citizens reported receiving the SMS late, while others reported being frightened or made nervous by the message content which was later considered to be over-the-top. In this particular trial, citizens were not warned about the impending message which meant that when they received it, hundreds of anxious citizens called triple zero concerned about the pending adverse weather conditions. While this is a typical response to interpreting instant messages during emergencies by a small portion of the population, more research needs to be done into effective and clear communications via mobile phones (Michael et al, 2006).

Queensland, in particular, faces the risks of cyclones, bushfires, storm surges and floods on an annual basis. In 2009, the Council of Townsville City started to provide an early warning service to its residents on an opt-in basis. The Early Warning Network (EWN) sends alerts 30

minutes ahead of severe weather conditions via a variety of electronic channels including email, SMS and landline phone call (Chudleigh, 2009). The cost of each message sent is borne by the Council. This system is believed to be the “the world’s only location based early warning system for severe weather events” with the ability to pinpoint the area that information is needed “with accuracy to within 10m” according to EWN managing director Mr. Kerry Plowright (The Australian Early Warning Network, 2009).

The National Emergency Warning System of Australia

Not until recently was the standardization of a national emergency planning and alerting approach to public warning across Australia considered for actual implementation. A national emergency warning system has been the subject of discussion between the Commonwealth, States and Territories since 2004. In 2005, there was a prevailing view of the need to introduce a warning system on a national level but it was not subject to agreement by all States and Territories (The Victorian Bushfires Royal Commission, 2009). However, by July 2008, the Council of Australian Governments (COAG) finally reached an agreement to establish a national telephone-based emergency warning system in Australia (The Australian Government: Attorney General’s Department, 2009). But according to the Prime Minister of Australia, privacy and data security restrictions in the *Telecommunications Act 1997* combined with interstate disagreements over funding schemes, delayed the system’s introduction till after the Victorian bushfires in February 2009 (Bita & Sainsbury, 2009).

New innovations are often subject to a multitude of social-ethical issues such as privacy and security concerns in their incubation period. In this instance, the changes needed to the Telecommunications Act were not made in a timely fashion thus stifling the roll out of the telephone based warning system. This is an example of where the law lags behind new technologies or services. Despite that this system was to merely send a message to a telephone, the appropriate legislative process had not taken place. Laws or amendments to current laws do not usually happen overnight. However, following the worst bushfire season in Australia’s history in 2009, the Federal Australian Government, COAG and the State and Territory Governments identified the compelling need for the immediate deployment of the national warning system which would enable them to deliver warnings to landline and mobile telephones based on the billing address of the subscriber (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009). It should be stressed here that after the Victorian Bushfires it only took several days for Honorable Senator John Faulkner, a Cabinet Secretary and Special Minister of the State, to sign the Emergency Bushfires Declaration No.1 on behalf of the Victorian Government. The declaration was made under Section 80J of the *Privacy Act 1988*. Section 80J is primarily concerned with the declaration of an emergency or an event of national significance and only the Prime Minister of Australia or the Minister of relevance may make such a declaration.

The National Emergency Warning System (NEWS) was operational in October 2009 in all States and Territories except Western Australia (WA) which delivered its emergency warning messages through the use of its own WA StateAlert system (The Victorian Department of Treasury and Finance, 2009). Under the COAG agreement, States and Territories retained autonomy of the warning systems they choose to implement (The Australian Government: Attorney General’s Department, 2009). NEWS is meant to supplement, and not to replace, the range of traditional measures currently used to warn the public of emergencies, including television and radio, public address systems, door knocking, sirens, signage and the internet (Gibbons, 2009).

Granting NEWS Stakeholders Access to the Integrated Public Number Database

The second stage of NEWS is presently under deliberation, in particular the ability for Australian telecommunications carriers to meet the long term requirements of a national emergency alerting and warning system utilizing location-based technologies to identify

active mobile handsets of all carriers within a defined emergency area (The Victorian Department of Treasury and Finance, 2009). For the first stage of NEWS to operate, access to the IPND was required in order to obtain the number and address upon which the warning is disseminated (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009). IPND is an industry-wide, commonwealth-owned database that contains all the residential and business telephone numbers, both listed and unlisted, and other subscriber information such as name, address, and the type of service delivered by each number (i.e. landline, fax, mobile, pager, etc.) (The Australian Communications and Media Authority, 2009). IPND was established and is maintained by Telstra, as a condition of its carrier license. All telecommunications carriers and service providers are required to provide Telstra with subscriber information in order to populate and maintain the database (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009). Maintaining accurate IPND data is extremely important to ESOs as these organizations rely on the IPND to respond to emergency calls from the public in a timely manner (The Australian Communications and Media Authority, 2009).

In accordance with the States and Territories agreement to establish NEWS, the Federal Government immediately commenced drafting legislation to authorize access to the IPND. This was not without some controversy, despite the obvious benefits of the new warning system, even the potential to save lives. Given the sensitive nature of the information contained in the IPND, the *Telecommunications Act 1997*, Sections 276 and 277, restricts access and prohibits disclosure or use of information from the database save for a few exceptions. These exceptions are explicitly specified in the legislation which allow for the release of personal information for a number of reasons including emergency calls, law enforcement and national security purposes (The Australian Communications and Media Authority, 2009).

In 2009, the Federal Government introduced into Parliament *the Telecommunications Amendment Integrated Public Number Database 2009 Bill* that proposed amendments to the *Telecommunications Act 1997* in order to enable access to the IPND for NEWS purposes, in connection with the provision of telephony-based emergency warnings and for the supply of location-based emergency services (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009).

In light of the Victorian Bushfires, the government sought advice from the Solicitor-General on an interim measure to allow immediate access to the IPND by any State or Territory that wished to implement a more limited system, as soon as possible. This interim access was not a substitute for the amendments to the Telecommunications Act contained in the Bill and the planned future access arrangements for the IPND (Gibbons, 2009), but some citizens and civil liberties groups did voice concern over the potential for breaches in information privacy. The amendments to the Telecommunications Act contain a number of privacy protection provisions, which are intended to ensure that subscriber data obtained from the IPND is not used or disclosed for any other purpose than to provide telephone-based emergency warnings. Specifically, emergency agencies will only be permitted to access the data in the event of an actual emergency, in the event of a likely emergency or for testing purposes (i.e. to test whether in the event of an emergency the alert would have reached the people that it needed to) (Gibbons, 2009).

The amendments provide the Attorney-General, as the Minister with portfolio responsibility for emergency management issues, with powers to specify, by legislative instrument, who can use IPND information in the event of an emergency or disaster (The Australian Government: Attorney General's Department, 2009). The amendments also contain accountability measures including a reporting requirement for any government agency that activates a telephony-based emergency warning using IPND data. The agency will be required to report each usage of IPND information to the Attorney-General and to the ACMA, as soon as

practicable after each incident occurs (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009). Agencies will be required to report on the nature and location of the emergency or disaster, the number of telephone numbers disclosed, the number of persons to whom the numbers were disclosed and why. Agencies will also be required to report annually to ACMA and to the Office of the Privacy Commissioner (OPC) on each disclosure (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009).

With regard to the location-based emergency services phase of NEWS, the bill clarifies the Telecommunications Act by explicitly allowing carriers and service providers supplying LBS to access listed public number information in the IPND, since the current Telecommunications Act does not contain express authority for use of information in the IPND for the purpose of providing LBS on a large scale (Gibbons, 2009). The Bill seeks to explicitly permit access to IPND data for the purpose of providing location-based emergency services and only limited to that information necessary to provide such services. The amendments also extend the existing secondary usage provisions of the Telecommunications Act to prohibit the use or disclosure of IPND data obtained for the purpose of providing the services, except for the purposes permitted under the Act. The prohibition against secondary usage applies to either the carrier or service provider, which initially requested the data and to any other party who may receive the information (The Australian Government: Department of Broadband Communications and the Digital Economy, 2009).

Location-Based Emergency Services in Australia

Unlike in the United States, technical feasibility in the context of location accuracy standards for emergency purposes does not yet exist in Australia. In addition, the commitments for telecommunications carriers are less restrictive since Australian regulators, primarily the ACMA, do not enforce accuracy levels on carriers (The Australian Communications and Media Authority, 2004). At present, a call from a mobile handset to an emergency call service is accompanied by very broad mobile location information (MoLI) relating to what is known as a standardized mobile service area (SMSA). These SMSAs can range in size from 2,000 to 500,000 square kilometers, according to the cell's size from where the emergency call is originated, and are thus too broad to assist ESOs to find someone in an emergency. Rather, the SMSAs are used by the emergency call person to identify the requested ESO answering point that is closest to his or her location, a process known as jurisdiction determination (The Australian Communications and Media Authority, 2004). Many aspects of these services are regulated and monitored by ACMA under the primary legislation, namely the *Telecommunications (Consumer Protection and Service Standards) Act 1999* and *Telecommunications Act 1997*, and through two subordinate legislative instruments: (i) *Telecommunications (Emergency Call Service) Determination 2002*; and (ii) *Telecommunications (Emergency Call Persons) Determination 1999* (The Australian Communications and Media Authority, 2004).

High accuracy location techniques to provide accurate MoLI in emergency situations are yet to be implemented in Australia but one future aim is to reach accuracy levels within 50 to 500 meters (The Australian Communications and Media Authority, 2004). Currently, location methods that can identify the mobile base station being used to carry an emergency handset call, thus providing MoLI generally within 500 meters to 30 kilometers of accuracy, are available and ready to be used in Australia but prior to 2009 were not extensively deployed by the country's telecommunications carriers (The Australian Communications and Media Authority, 2004). However, this is expected to change as the feasibility of high accuracy location methods are currently under investigation after the Federal Australian Government, Council of Australian Governments (COAG) and the States and Territories identified the compelling need for this technology in Australia, following the tragic 2009 bushfires (The Victorian Bushfires Royal Commission, 2009).

Accordingly, in regard to the second type of location-based emergency service application, which is initiated by government agencies to people in the event of an emergency, the Victorian Government released a tender in August 2009 on behalf of COAG. The tender sought responses for the purpose of determining the capacity and capability of the Australian telecommunications carriers in meeting the long term future requirements for a national emergency alerting and warning system utilizing location-based technologies to identify the active mobile handsets of all carriers, within a defined emergency area (The Victorian Department of Treasury and Finance, 2009). The tender document envisaged the underlying technology to be capable of the following:

1. The technology will have the ability to receive notifications about any new mobile device entering a previously specified emergency area to alert the user that, for example, an emergency services vehicle has arrived at a location, or a civilian has entered the area and may be unaware of the emergency.
2. The technology will include the ability to receive notifications for any mobile device exiting the defined emergency area. This could facilitate the creation of an evacuation list of people who are still remaining in the emergency area.
3. The technology will be able to locate specific mobile devices in both 2G and 3G networks, and overlay their position onto a map.
4. The technology will have the ability to provide sufficient privacy and authentication checking mechanisms to ensure mobile location security (The Victorian Department of Treasury and Finance, 2009)

SOCIO-ETHICAL CONSIDERATIONS

The location-based emergency warning system should allow the government to determine the almost exact geographic coordinates of all active mobile handsets in a defined emergency area(s) or locate mobile handsets in real time within specific threatened zone(s), and then to disseminate, and be able to re-disseminate when necessary, a warning message to these mobile handsets. Determining and/or locating the mobile handset whereabouts does not necessarily require an explicit consent from its user as pertinent government departments and law enforcement agencies have the power, under the *Privacy Act 1988*, to temporarily waive the person's right to privacy in emergencies based on the assumption that the consent is already implied in such situations.

It is quite true that emergencies do represent unique contexts where privacy is most likely to be one of our least concerns. In theory, the location/determination processes cannot trigger concerns being employed specifically for emergency management, but the perception of the uninterrupted availability of these technologies in the hands of governments during normal daily life situations has the potential to raise concerns about the possibility of utilizing them for other purposes, specially under a one-year long emergency declaration. In addition, the implications of waiving away the consent, even temporarily, has the power to impact adversely on the individual's trust in the government and its mandated LBS solutions. These concerns have the potential to add impetus to the ongoing debate of how much individuals are truly willing to relinquish their right to privacy in exchange for a sense of continuous security. This is especially now true in the current political climate of the so-called "war on terror" where governments have started to bestow additional powers on themselves to monitor, track and gather personal information in a way that never could have been previously justified (Perusco & Michael, 2007). In the name of national security, such measures have become justified albeit in exceptional situations. Despite being beyond the established rule of law these exceptions are now considered an absolute necessity to maintain the security of society and its interdependent critical infrastructures (Cavelty, 2007).

When location-based services are employed by governments the individual may never know the true extent of the location/determination on his or her handset's whereabouts or the

breadth of location information being collected. Location information is a particularly sensitive kind of personal information that can have intrusive consequences on individual lives if misused (The Australian Communications and Media Authority, 2004). This kind of information can be collected, stored, aggregated and when correlated with other personal information a broad view of behavioral patterns or detailed portraits of individual habits can be created (Clarke & Wigan, 2008; Parenti, 2003). One need only ponder on what personal data is available on social networking sites. Nicola Green posited that location-based technologies might be used one day to hold individuals institutionally accountable for their day-to-day activities (2001). In his work about location-based profiling, Ronald Leenes provides two cases of where location data was used in criminal investigations (2008). Indeed, this profiling of individuals is what makes people uneasy about LBS being in the hands of governments, because of concerns about privacy in general as well as fears of being incorrectly profiled (Holtzman, 2006). Consider the sensitivity of location information pertaining to minors or the elderly who are vulnerable in different ways, or those persons suffering from mental illness.

In this age of “permanent emergency” (Parenti, 2003), perhaps now more than ever, LBS do emerge as promising technologies that can add significant value to the all-hazards approach governments are advocating in national security. Nonetheless, a transparent society where privacy is completely abolished by governments in the name of security is neither feasible nor acceptable. This is because of the inherent value of privacy for both the individual and society (Schneier, 2008). Privacy is indispensable in a community that recognizes social freedom as good and where many people dislike exposure of their private actions not because they have acted irregularly but because their psychological nature requires privacy (Ben-Ze'ev, 2003). Accordingly, governments have to incur an ethical obligation of defining clear limits on privacy intrusions if these intrusions are to be framed in the name of security. Harkin (2003) raised this issue when he stated that “unless there are clear limits on how government can employ the information that it gleans from our mobile communications – and in the current climate of international terrorism, few governments are keen to impose limits on their own meddling – there may well be a backlash that will impede the development of the technology itself”.

Requirements for Location-based Emergency Systems: Equity and Access

Location-based emergency systems are part of all-hazard alert and warning systems that include other emergency notification mechanisms (The Federal Communications Commission, 2005). Several national authorities, international standards organizations, and a number of specialist researchers have undertaken extensive studies to identify and document different requirements for different public emergency warning systems that should in principle allow support for all current and future emergency event types. In these studies, many aspects were given attention, including legislative, regulatory, administrative, operational, technical, organizational and ethical requirements. Some of these contributions have been by Mileti and Sorensen (1990), the Cellular Emergency Alert Systems Association (2002), ETSI (2003; The European Telecommunications Standards Institute, 2006a, 2006b, 2010), Tsalgatidou et al. (2003), FCC (2005), McGinley et al. (2006), the International Telecommunications Union (2007), The 3rd Generation Partnership Project (2008; The 3rd Generation Partnership Project, 2009), Fernandes (2008), The Victorian Bushfires Royal Commission (2009), The Victorian Department of Treasury and Finance (2009), and Jagtman (2009), Sanders (2009), and Setten and Sanders (2009) under the European Commission's CHORIST Project (2009).

In general, defining requirements serves several objectives such as establishing a standardized way of developing and implementing a system, prioritizing the system's future functionality while providing guidance on the system's expected performance levels, preventing duplicative reporting for the system's stakeholders (The United States Department of Homeland Security, 2008), and ensuring that people who want access to LBS services during

emergencies can have them in addition to other mechanisms they have traditionally enjoyed. With regard to location-based emergency systems, no explicit requirements, specifically legal and administrative requirements, currently exist anywhere in the world (Togt, Beinat, Zlatanova, & Scholten, 2005). Nonetheless, based on the concepts and principles outlined in the above-mentioned works, the following specific requirements have been drawn from the literature for location-based emergency warning and alerting systems. These requirements include, but are not limited to:

1. Ability to be integrated or used along with other alerting and warning systems.
2. Be fully accessible to the right authorities.
3. Be only accessible by the right authorities.
4. Be flexible to allow support for all current and future types or categories of emergency events and not to be designed to support specific type(s) of emergencies or events requiring notification.
5. Ability to operate independently of a specific telecommunications carrier network.
6. The underlying technology should be supported by all telecommunications carriers in the country.
7. Be able to accommodate newer technologies to enable futuristic enhanced transfer modes (e.g. messages with large data content such as video within the warning notification in order to send, for example, a map of safe area or emergency facilities).
8. Have the ability to provide sufficient privacy and authentication checking mechanisms to ensure mobile location security.
9. Support both pre-planned and dynamic notification events.
10. Reach an unrestricted number of people, ranging from hundreds in rural areas to millions in urban and metropolitan cities.
11. Deliver messages simultaneously to a large number of recipients.
12. Deliver the message in near real-time or within a planned specified time.
13. Reach the appropriate recipients, as efficiently as possible, through the ability of the underlying technology to segment the message recipients by geographic locations.
14. Allow the opportunity to send different messages to different groups of people (e.g. recommend different safety areas for different groups or messages can be targeted at people in the immediate vicinity of an emergency to do one thing, and people traveling to an affected area to do another).
15. Reach all kinds of existing mobile handsets including legacy devices that are largely still in use.
16. Support delivery of messages to those with special needs and unique devices, such as handsets for hearing and vision impaired persons.
17. Reach the residents of remote areas, and people roaming from other mobile telecommunications networks, including visitors from other countries.
18. Support the transmission in languages in addition to English to the extent where it is practical and feasible.
19. Be able to deliver the message under network-congested conditions.
20. Have a message redelivery mechanism when the initial message delivery fails.
21. Have a message reiteration mechanism for as long as the message is valid.

In addition to the base requirements for the location-based emergency system, the requirements for the service/message itself should consider, but are not limited to, the following:

1. Message creation is driven by the country's specific characteristics and its own list of emergencies.
2. Message template is consistent across different warning sources from different emergency authorities.
3. Message is based on standardized digital format for expressing and disseminating a consistent warning message simultaneously over different informative and media channels.

4. Specifically recognizable as being an emergency message that cannot be mistaken for an ordinary message.
5. Credible, secure and authentic.
6. Location-specific, to minimize social anxiety.
7. Relevant, to ensure that recipients realize that the warning relates to their personal situation.
8. Timely, to prevent wrong actions and to provide those at risk with enough time to take protective action.
9. Accurate, to indicate the degree severity, or the predicted severity, of the event.
10. Complete, to offer sufficient details about the situation.
11. Concise, to avoid lengthy messages.
12. Provide adequate instructions to recipients regarding what should and should not be done to protect them.
13. Fully clear and comprehensible to all people including young and senior recipients.
14. Positive, rather than negative to advocate people on what to do.

One of the greatest threats to such service implementation comes from the potential for instant message hoaxes during times of crisis (i.e., disinformation) from unscrupulous citizens to other unsuspecting citizens, as was reported in the fight against SARs (Severe Acute Respiratory Syndrome) in Hong Kong in 2003 (Jardin, 2003). These are not only disruptive to emergency services but can also be life-threatening to individuals who are misinformed. There is unfortunately little authorities can do to guard against such communications.

OVERCOMING EMERGENCY ALERT SHORTCOMINGS

During an emergency, traditional standard emergency warning signal (SEWS) techniques are reliable and dependable because they are easily recognized and trusted by members of the public (Ministry for Police and Emergency Services, 2011). For example, in Australia, the Australian Broadcasting Corporation (ABC) has aired radio and television campaigns for decades that have noted that it is the local “emergency services broadcaster” that citizens need to pay attention to and act accordingly in response. These SEWS services are considered authentic because they reach a mass target audience at exactly the same time, and are coming from a source feed that is difficult to corrupt. With newer emergency warning systems being introduced relying on personal devices like a mobile telephone SMS or fixed line voicemail, human factors and system design issues can become significant problems (Jean, 2011; 2012). Citizens who receive a text message from authorities such as the police, about an impending emergency which does not eventuate are likely to take subsequent messages to their phone less seriously. This is analogous to Aesop’s fable, “The Boy Who Cried Wolf.” The other problem till now with regards to mobile alerts has been the over-reliance on someone’s billing address details to receive a message about an emergency (Hilvert, 2011). This has led to some strange happenings where people who are overseas receive a text message about an emergency that is occurring in their home town many thousands of kilometers away.

Consider the case where an emergency alert is sent out to citizens and riddled with spelling errors. One such example occurred in the chemical fire emergency in the Australian Capital Territory (ACT) in the suburb of Mitchell (Humphries, 2011; Ludwig, 2011). Citizens received a text message on September 16, 2011 in the early hours of the morning, which read: “Emergency. Emergency. The ACT Fire Brigade is responding to a Chemical insadent in Mitchell. Resadents are advised to evacuate the suburb immediately.” Such experiences decrease citizen confidence in critical emerging systems deployed by the government. This is despite the fact that the error did not come down to someone who could not spell or who rushed through the system an unchecked message. But rather an officer who reused a phonetically-spelled text destined for a text-to-speech recognition system to also reach out to citizens via SMS. It is still unclear whether the Mitchell incident was a systems design error, or human error based on poor training, or poor implementation of the guidelines for sending out such mobile alerts. Emergency Services Agency Commissioner Mark Crosweller went on

record openly declaring his agency had made some mistakes during the Mitchell incident. He said: “[w]e've assessed the way that we used the system, we've improved our procedures, we've improved our training and we've made recommendations back to the system's operator about improving the user interface” (Jean, 2011).

Several other problems plagued the emergency alert system during the Mitchell fire in the ACT which used the fifteen million dollar system instituted on December 1, 2009. Primarily, insufficient time was allocated to allow the system to dial all of the numbers in the target area. In an inquiry following the fire, Attorney-General Robert McClelland stated that the emergency alert system had simply not been used correctly. For instance, authorities made 30,530 calls to 86,801 landlines within the first 30 minutes of the fire and of those only 13,784 were answered. In essence, only about a third of the landline numbers could be dialed within thirty minutes. Authorities also sent text messages to more than 52,700 mobile phones, of a total pool of 83,774 mobiles. Despite the emergency alert system used in the Mitchell fire had previously been deployed successfully in Canberra in 2003, and had been previously used 329 times to send 7.12 million messages, this time it failed in its execution (Jean, 2011; Hilvert, 2011). What the Mitchell fire did demonstrate however was the need to steer away from the use of the IPND billing address to a location-based mobile telephone emergency warning system (Environment and Sustainable Development Directorate, 2011). During the fire, the data source for Emergency Alert, the Location Based Number Store (LBNS) came directly from the IPND. The Emergency Alert system was designed to send 1,000 voice messages and 30,000 SMS per minute.

In two other notable incidences where an older emergency alert system was brought into question included the March 30, 2009, Sydney City power failure which affected over 100,000 people. SMS text messages were sent to building managers and site coordinators in the city using the SydneyAlert system, over an hour after the power went down (Robinson, 2012). Employees in 34 tall buildings walked down evacuation stairwells in near darkness without any knowledge of what had occurred. Some suspected a terrorist attack, and were none the wiser as they exited onto the main city streets, only to find 137 intersections with traffic lights that were blank. To add to the confusion, 98 loudspeakers that had been installed to a value of two million dollars were not working, and there was no backup battery generator, so that at least people knew what they had to do. It was up to the Fire Brigade to keep people moving and make their way home.

Prior to this incident on March 2, 2009, Victorian police also used SMS to reach about 5 million mobile phone customers with a message that read: “Extreme weather in VIC expected Mon night and Tues. High wind & fire risk. Listen to Local ABC Radio for emergency updates. Do not reply to this msg” (Schulz, 2009). It is important to note that some members received their SMS several days after it was meant to reach them. In addition, so concerned were some citizens by the directness of the communications, that some anxiously called triple-zero seeking further information. What transpired was not an emergency at all, and so some citizens felt misled by the SMS authorized by the Police.

Enter the possibility of utilizing the Internet for emergency alerting (e.g. Twitter and other microblogging and social networking engines), and one can see how quickly a paradigm shift will be required to enable the new location-based techniques that have been promised in Australia since the Victorian Bushfires. At the beginning of January 2012, the Victorian Government (acting on behalf of all the States and Territories in Australia), entered into a contract with Telstra to provide location-based real-time alerts during emergencies. This means that in future emergency alerts, only people who are in an affected area will be notified of an emergency, and not just those whose billing details are designated in the affected area. Initially only mobile phone users subscribed to Telstra will receive these messages, but the Victorian Government has stepped up its efforts to form contractual agreements with the other two major mobile service providers, Optus and Vodafone (Lee, 2012).

Time and time again, emergency ministers have emphasized that the new technologies should be used in concert with traditional SEWS techniques. We might be getting more sophisticated in how we target citizens for emergency alerting through location-based services, but we still need to emphasize the importance of following due process for government agencies and emergency service organizations (eGov, 2012).

CONCLUSION

Large scale emergencies, that have the potential to disrupt the orderly manner of civil society, are now considered a type of national security challenge. While there is a growing trend by governments to deploy more socially constructed security measures to counter the threatening consequences of extreme events, the public reception has not always been favorable. In Australia, some citizens and lobby groups see the introduction of laws mandating access to certain types of personal information to aid in the gradual relinquishing of individual privacy rights. Beyond unauthorized access and disclosure of citizen personal details is the public perception that authorities will be able to perform continuous tracking after legitimately deploying a one year long emergency declaration. With a limited effort from the government to raise public awareness about the deployed system, most of the concerns, although they may merely be misconceptions, have the power to impact negatively on the practiced emergency response measures while devaluing the purpose of the alert and warning system in the eyes of the public. The time to intervene is now as governments, like Australia, move to introduce basic systems moving to more sophisticated and fully-fledged location based services into the future. It is important for governments, telecommunications carriers and relevant stakeholders to discuss the possible socio-ethical implications of advanced technologies like location based services before they are rolled out in a ubiquitous manner. In trying to respond to the challenge of national security, governments will ironically need to invest even more money into such areas as database security to ensure that private citizen details are not disclosed to unauthorized parties.

REFERENCES

- ABC News. (2009, Mar 4, 2009). Bushfire SMS to Assist in Warning System Development. *The Australian Broadcasting Corporation*.
- Aitenbichler, E. (2008). A Focus on Location Context. In M. Mühlhäuser & I. Gurevych (Eds.), *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises* (1st ed., pp. 257-281). Hershey, Pennsylvania: IGI Global.
- Astroth, J. (2003). Location-Based Services: Criteria for Adoption and Solution Deployment. In B. E. Mennecke & T. J. Strader (Eds.), *Mobile Commerce: Technology, Theory, and Applications* (pp. 229-236). Hershey, Pennsylvania: Idea Group Publishing.
- Australia.gov.au Website. (2010). *The Australian Continent*. Retrieved 10 March 2010. from <http://australia.gov.au/about-australia/our-country/the-australian-continent>.
- Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, 19(4), 451-467.
- Benson, S. (2007). SMS Smog Alerts for Sydney. Retrieved 7 June 2007, Factiva
- Bernardos, A. M., Casar, J. R., & Tarrío, P. (2007). *Building a framework to characterize location-based services*. Paper presented at the Conference Namel. Retrieved Access Datel. from URLl.

- Betts, R. (2003). The Missing Links in Community Warning Systems: Findings from Two Victorian Community Warning System Projects. *The Australian Journal of Emergency Management*, 18(3), 35-45.
- Bitá, N., & Sainsbury, M. (2009). Bungling Silenced Victoria Bushfires Warning. *The Australian*.
- Boughton, G. (1998). The Community: Central to Emergency Risk Management. *Australian Journal of Emergency Management*, 2-5.
- Buzan, B., Wver, O., & Wilde, J. D. (1998). *Security: A New Framework for Analysis* (1st ed.). London: Lynne Rienner Publishers.
- Canton, L. G. (2007). *Emergency Management: Concepts and Strategies for Effective Programs* (1st ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.
- Cavelty, M. D. (2007). Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*, 4(1).
- Chudleigh, J. (2009, November 10, 2009). Earlier Alert System for Severe Weather. *The Courier-Mail*.
- Clarke, R., & Wigan, M. (2008). You are where you have been. In K. Michael & M. G. Michael (Eds.), *Australia and the New Technologies: Evidence Based Policy in Public Administration* (pp. 100-114). Canberra: University of Wollongong.
- Coyle, D., & Meier, P. (2009). *New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks*. Retrieved 24 December 2009. from.
- Dawson, M., Winterbottom, J., & Thomson, M. (2007). *IP Location* (1st ed.). New York: McGraw-Hill.
- Dobbin, M. (2009, March 3, 2009). Victorians Receive Fire Text Warning. *The Age*.
- Dunn, M., & Collier, K. (2007, February 27, 2007). Plan to use SMS for SOS. Retrieved 6 June 2007, Factiva
- eGov. (2012). Emergency Alerts and Warnings - Australia. *eGovernment Resource Centre* Retrieved June 15, 2012, from <http://www.egov.vic.gov.au/focus-on-countries/australia/government-initiatives-australia/emergencies-and-safety-australia/emergency-alerts-and-warnings-australia.html>
- Emergency Management Australia. (1996). *Australian Counter Disaster Handbook* (5th ed. Vol. 2). Canberra, Australia: Emergency Management Australia.
- Emergency Management Australia. (2004a). *Disaster Recovery: Safer Sustainable Communities*. Retrieved 27 November 2007. from [http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/\(3273BD3F76A7A5DED AE36942A54D7D90\)~Manual10-Recovery.pdf/\\$file/Manual10-Recovery.pdf](http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/(3273BD3F76A7A5DED AE36942A54D7D90)~Manual10-Recovery.pdf/$file/Manual10-Recovery.pdf).
- Emergency Management Australia. (2004b). *Emergency Management in Australia: Concepts and Principles*. Retrieved 27 November 2007. from [http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/\(3273BD3F76A7A5DED AE36942A54D7D90\)~Manual01-EmergencyManagementinAustralia-ConceptsandPrinciples.pdf/\\$file/Manual01-EmergencyManagementinAustralia-ConceptsandPrinciples.pdf](http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/(3273BD3F76A7A5DED AE36942A54D7D90)~Manual01-EmergencyManagementinAustralia-ConceptsandPrinciples.pdf/$file/Manual01-EmergencyManagementinAustralia-ConceptsandPrinciples.pdf).

- Emergency Management Australia. (2008). Disasters Database. Retrieved 04 January 2008, from http://www.ema.gov.au/www/emaweb/emaweb.nsf/Page/Resources_DisastersDatabase_DisastersDatabase
- Emergency Management Australia. (2009a). *Australian Emergency Management Arrangements*. Retrieved 27 November 2009. from [http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/\(3A6790B96C927794AF1031D9395C5C20\)~Australian+Emergency+Management+Arrangements.pdf/\\$file/Australian+Emergency+Management+Arrangements.pdf](http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)~Australian+Emergency+Management+Arrangements.pdf/$file/Australian+Emergency+Management+Arrangements.pdf).
- Emergency Management Australia. (2009b). Emergency Management. Retrieved 08 December 2008, from http://www.ema.gov.au/www/emaweb/emaweb.nsf/Page/Emergency_Management
- Environment and Sustainable Development Directorate. (2011). Ministerial Statement- Mitchell Fire. Retrieved September 20, 2011, from http://www.environment.act.gov.au/_data/assets/pdf_file/0009/232299/Ministerial_Statement_on_Mitchell_fire,_20_September_2011.pdf
- European Commission. (2011). Satellite Navigation: Why Galileo? Retrieved 11 January 2012, from http://ec.europa.eu/enterprise/policies/satnav/galileo/why/index_en.htm
- European Space Agency. (2011). What Is Galileo? Retrieved 11 January 2012, from <http://www.esa.int/esaNA/galileo.html>
- Fernandes, J. P. (2008). Emergency Warnings with Short Message Service. In H. G. Coskun, H. K. Cigizoglu & M. D. Maktav (Eds.), *Integration of Information for Environmental Security* (1st ed., pp. 205-210). Dordrecht, The Netherlands: Springer.
- Gibbons, S. (2009). *Telecommunications Amendment (Integrated Public Number Database) Bill 2009: Second Reading*. Retrieved 6 August 2009. from http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2009-02-26/0032/hansard_frag.pdf;fileType=application%2Fpdf.
- Gilbert, C. (1998). Studying Disaster: Changes in the Main Conceptual Tools. In E. L. Quarantelli (Ed.), *What is a Disaster? A Dozen Perspectives on the Question* (1st ed., pp. 3-12). New York: Routledge.
- Green, N. (2001). Who's watching whom? Monitoring and accountability in mobile relations. In B. Brown, N. Green & R. Harper (Eds.), *Wireless world: social and interactional aspects of the mobile age* (1st ed., pp. 32 - 45). New York City: Springer-Verlag.
- Grothe, M. J. M., Landa, H. C., & Steenbruggen, J. G. M. (2005). The Value of Gi4DM for Transport & Water Management. In P. v. Oosterom, S. Zlatanova & E. M. Fendel (Eds.), *Geo-information for Disaster Management* (1st ed., pp. 129-154). Delft, The Netherlands: Springer.
- Gruber, B., & Winter, S. (2002). *Location Based Services using a Database Federation*. Paper presented at the 5th AGILE Conference on Geographic Information Science, Palma, Spain.

- Guan, J., Zhou, S., Zhou, J., & Zhu, F. (2007). Providing Location-Based Services under Web Services Framework. In D. Taniar (Ed.), *Encyclopedia of Mobile Computing and Commerce* (1st ed., pp. 789-795). London: Information Science Reference.
- Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2006). *Introduction to Emergency Management* (2nd ed.). Burlington, Massachusetts: Elsevier Butterworth-Heinemann.
- Harkin, J. (2003). *Mobilisation: The growing public interest in mobile technology* (1st ed.). London: Demos.
- Harvey, F. (2008). *A Primer of GIS : Fundamental Geographic and Cartographic* (1st ed.). New York City: The Guilford Press.
- Hilvert, J. (2011). Dodgy text tarnishes SMS emergency service system. *ITNews* Retrieved September 23, 2011, from http://www.itnews.com.au/promos/interstitial/interstitial_dfp.html?l=10;KnvJuy7QTzEfzPKF8zesJyG8le2WW6.qtlJDF2ITieqTGRqifR;http%3A%2F%2Fwww.itnews.com.au%2FNews%2F272863%2Cdodgy%2Dtext%2Dtarnishes%2Dsms%2Demergency%2Dservice%2Dsystem.aspx
- Hjelm, J. (2002). *Creating Location Services for the Wireless Web* (1st ed.). New York: John Wiley & Sons, Inc.
- Holma, H., Kristensson, M., Salonen, J., & Toskala, A. (2004). UMTS Services and Applications. In H. Holma & A. Toskala (Eds.), *WCDMA FOR UMTS: Radio Access for Third Generation Mobile Communications* (3rd ed., pp. 11-46). West Sussex, England: John Wiley & Sons Ltd.
- Holtzman, D. H. (2006). *Privacy Lost: How Technology Is Endangering Your Privacy* (1st ed.). San Francisco, California: Jossey-Bass.
- Humphries, G. (2011). Attorney-General: Emergency Alert (Question No. 1434). *Senate Debates* Retrieved 22 November, 2011, from <http://www.openaustralia.org/senate/?id=2011-11-22.155.1>
- Ife, H. (2009, March 02, 2009). Texts Alert Victorians of Fire Danger. *Herald Sun*.
- Jagtmann, E. (2009). *Reaching Citizens with CHORIST: Everything but Technology*. Retrieved 18 October 2009. from <http://www.chorist.eu/index.php?page=1&sel=1>.
- Jardin, X. (2003). Text Messaging Feeds SARS Rumors, *Wired*. Retrieved 17 October 2009, from <http://www.wired.com/medtech/health/news/2003/04/58506>.
- Jean, P. (2011). Govt rebuked over Mitchell fire response. Retrieved November 23, 2011, from <http://www.canberratimes.com.au/act-news/govt-rebuked-over-mitchell-fire-response-20111123-1v2u0.html>
- Jean, P. (2012). SMS alert system is short on delivery. *The Age* Retrieved February 29, 2012, from <http://m.theage.com.au/act-news/sms-alert-system-is-short-on-delivery-20120228-1u187.html>

- Jensen, C. S. (2002, 08-11 January). *Research Challenges in Location-Enabled M-Services*. Paper presented at the Third IEEE International Conference on Mobile Data Management, Singapore.
- Kaplan, E. D., & Hegarty, C. J. (2006). *Understanding GPS: Principles and Applications* (2 ed.). Norwood, Massachusetts: Artech House.
- Küpper, A. (2005). *Location-Based Services: Fundamentals and Operation* (1st ed.). Chichester, West Sussex: John Wiley & Sons Ltd.
- Lee, M. (2012). Telstra adds location to emergency alerts *ZDNet* Retrieved January 13th, 2012 from <http://www.zdnet.com.au/telstra-adds-location-to-emergency-alerts-339329657.htm>
- Leenes, R. (2008). Reply: Mind My Step? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (1st ed., pp. 160-168). Dordrecht, The Netherlands: Springer.
- Lopez, X. R. (2004). Location-Based Services. In H. A. Karimi & A. Hammand (Eds.), *Telegeoinformatics: Location-Based Computing and Services* (1st ed., pp. 144-159). New York: CRC Press LLC.
- Ludwig, J. (2011). Attorney-General: Emergency Alert (Question No. 1434). *Senate Debates* Retrieved 22 November, 2011, from <http://www.openaustralia.org/senate/?id=2011-11-22.155.1>
- McClelland, R. (2011). Australia's Emergency Alert System Working Well. *ALP* Retrieved September 1, 2011, from <http://www.alp.org.au/federal-government/news/australia-s-emergency-alert-system-working-well/>
- McGinley, M., Turk, A., & Bennett, D. (2006). *Design Criteria for Public Emergency Warning Systems*. Paper presented at the The 3rd International Conference on Information Systems for Crisis Response and Management (ISCRAM), Newark, New Jersey.
- Michael, K, Stroh, B, Berry, O, Muhlhauber, A & Nicholls, T. (2006). The AVIAN Flu Tracker - a Location Service Proof of Concept, Recent Advances in Security Technology: Proceedings of the 2006 RNSA Security Technology Conference, Australian Homeland Security Research Centre, Canberra, 19-21 September, 244-258.
- Mileti, D. S., & Sorensen, J. H. (1990). *Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment*. Retrieved 08 August 2007. from <http://emc.ornl.gov/EMCWeb/EMC/PDF/CommunicationFinal.pdf>.
- Ministry for Police and Emergency Services. (2011). Standard Emergency Warning Signal (SEWS). Retrieved 21 January 2011, from <http://www.emergency.nsw.gov.au/sews>
- New South Wales Government. (2007). About sydneyALERT. Retrieved 17 April 2008, from <http://www.sydneyalert.nsw.gov.au/content.php/36.html>

- Oh, J., & Haas, Z. J. (2007). A Scheme for Location-Based Internet Broadcasting and Its Applications. *IEEE Communications Magazine*, 45(11), 136 - 141.
- Parenti, C. (2003). *The Soft Cage: Surveillance in America From Slavery to the War on Terror* (1st ed.). New York: Basic Books.
- Perry, R. W. (2007). What Is a Disaster? In H. a. Rodr'iguez, E. L. Quarantelli & R. Dynes (Eds.), *Handbook of Disaster Research* (1st ed., pp. 1-16): Springer Science+Business Media, LLC.
- Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: Evaluating location-based services. *IEEE Technology and Society Magazine*, 26, 4-16.
- Quarantelli, E. L. (1986). What Should We Study? Questions and Suggestions for Researchers About the Concept of Disasters. *International Journal of Mass Emergencies and Disasters*, 5(1), 7-32.
- Robinson, G. (2009). Warning: doubts over Sydney's alarm system. *smh.com.au* Retrieved March 31, 2009, from <http://www.smh.com.au/national/warning-doubts-over-sydneys-alarm-system-20090331-9hmg.html>
- Rosenthal, U. (1998). Future Disasters, Future Definitions. In E. L. Quarantelli (Ed.), *What is a Disaster? A Dozen Perspectives on the Question* (1st ed., pp. 147-160). New York: Routledge.
- Samsioe, J., & Samsioe, A. (2002). Introduction to Location Based Services: Markets and Technologies In R. Reichwald (Ed.), *Mobile Kommunikation: Wertschöpfung, Technologien, neue Dienste* (pp. 417-438). Wiesbaden, Germany: Gabler.
- Sanders, P. (2009). *The CB Way Forward*. Retrieved 18 October 2009. from <http://www.chorist.eu/index.php?page=1&sel=1>.
- Schneier, B. (2008). The Myth of the 'Transparent Society'. *Wired Magazine*.
- Schulz, M. (2009). Emergency services admit SMS bushfire alerts not foolproof. *Herald Sun* Retrieved March 03, 2009, from <http://www.heraldsun.com.au/news/more-news/emergency-services-admit-sms-bushfire-alerts-not-foolproof/story-e6frf7kx-1111119016715>
- Setten, W. v., & Sanders, P. (2009). *Citizen Alert with Cell Broadcasting:: The Technology, the Standards and the Way Forward*. Retrieved 18 October 2009. from <http://www.chorist.eu/index.php?page=1&sel=1>.
- Shiode, N., Li, C., Batty, M., Longley, P., & Maguire, D. (2002). The Impact and Penetration of Location-Based Services (pp. 1-16). London: Centre for Advanced Spatial Analysis, University College London.
- Spiekermann, S. (2004). General Aspects of Location-Based Services. In J. Schiller & A. Voisard (Eds.), *Location-Based Services* (1 ed., pp. 9-26). San Francisco, California: Elsevier.
- Stojanović, D., Djordjevic-Kajan, S., Papadopoulos, A. N., & Nanopoulos, A. (2007). Monitoring and Tracking Moving Objects in Mobile Environments. In D. Taniar

(Ed.), *Encyclopedia of Mobile Computing and Commerce* (1st ed., pp. 660-665). London: Information Science Reference.

- Templeman, D., & Bergin, A. (2008). *Taking a Punch: Building a More Resilient Australia*. Retrieved 02 February 2009. from http://www.aspi.org.au/publications/publication_details.aspx?ContentID=165.
- The 3rd Generation Partnership Project. (2008). *Technical Specification Group Services and System Aspects: Study for Requirements for a Public Warning System (PWS) Service (Release 8)*. Retrieved 13 Apr 2009. from http://www.3gpp.org/ftp/tsg_sa/WG1_Serv/TSGS1_37_Orlando/Docs/S1-070824.doc.
- The 3rd Generation Partnership Project. (2009). *Technical Specification Group Services and System Aspects; Functional Stage 2 Description of Location Services (LCS) (Release 9)*. Retrieved 16 January 2010. from http://www.3gpp.org/ftp/Specs/archive/23_series/23.271/.
- The Australian. (2007, February, 26 2007). Premier Promises Mobile Phone Terrorism Alert. Retrieved 7 June 2007, Factiva
- The Australian Communications and Media Authority. (2004). *Location Location Location: The Future Use of Location Information to Enhance the Handling of Emergency Mobile Phone Calls*. Retrieved 21 October 2007. from http://acma.gov.au/webwr/consumer_info/location.pdf.
- The Australian Communications and Media Authority. (2009). *Australia's Emergency Call Service in a Changing Environment*. Retrieved 25 September 2009. from http://www.acma.gov.au/webwr/assets/main/lib311250/future_of_emergency_call_services.pdf.
- The Australian Early Warning Network. (2009). Townsville City Council signs up to the Early Warning Network. Retrieved 7 December 2009, from http://www.ewn.com.au/media/townsville_city_council.aspx
- The Australian Government: Attorney General's Department. (2009). *Rudd Government Implements COAG Agreement on Telephone-Based Emergency Warning Systems (Joint Media Release)*. Retrieved 02 August 2009. from http://www.ag.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2009_FirstQuarter_23February2009-RuddGovernmentImplementsCOAGAgreementonTelephone-BasedEmergencyWarningSystems.
- The Australian Government: Department of Broadband Communications and the Digital Economy. (2009). *Telecommunications Amendment (Integrated Public Number Database) Bill 2009: Explanatory Memorandum*. Retrieved 6 August 2009. from [http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4062_ems_d2937505-3da9-4059-b9cb-e382e891dd23/upload_word/TelAm\(IPND\)_EM.doc;fileType=application%2Fmsword](http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4062_ems_d2937505-3da9-4059-b9cb-e382e891dd23/upload_word/TelAm(IPND)_EM.doc;fileType=application%2Fmsword).
- The Australian Government: Department of Transport and Regional Services. (2004). *Natural Disasters in Australia: Reforming Mitigation, Relief and Recovery Arrangements*.

Retrieved 18 February 2009. from
[http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/\(99292794923AE8E7CBABC6FB71541EE1\)~Natural+Disasters+in+Australia+-+Review.pdf/\\$file/Natural+Disasters+in+Australia+-+Review.pdf](http://www.ema.gov.au/www/emaweb/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~Natural+Disasters+in+Australia+-+Review.pdf/$file/Natural+Disasters+in+Australia+-+Review.pdf).

The Cellular Emergency Alert Systems Association. (2002). *Handset Requirements Specification: Reaching Millions in a Matter of Seconds*. Retrieved 02 April 2007. from http://www.ceasa-int.org/library/Handset_Requirements_Specification.pdf.

The European Commission. (2009). *The CHORIST Project: Integrating Communications for Enhanced Environmental Risk Management and Citizens Safety*. Retrieved 07 November 2009. from <http://www.chorist.eu/index.php?page=1&sel=1>.

The European Telecommunications Standards Institute. (2003). *Requirements for Communication of Citizens with Authorities/Organizations in Case of Distress (Emergency Call Handling)*. Retrieved 10 May 2007. from <http://etsi.org/WebSite/homepage.aspx>.

The European Telecommunications Standards Institute. (2006a). *Analysis of the Short Message Service and Cell Broadcast Service for Emergency Messaging Applications; Emergency Messaging; SMS and CBS*. Retrieved 10 May 2007. from <http://etsi.org/WebSite/homepage.aspx>.

The European Telecommunications Standards Institute. (2006b). *Emergency Communications (EMTEL): Requirements for Communications from Authorities/Organizations to Individuals, Groups or the General Public During Emergencies*. Retrieved 10 May 2007. from <http://etsi.org/WebSite/homepage.aspx>.

The European Telecommunications Standards Institute. (2010). *Study for Requirements for a Public Warning System (PWS) Service*. Retrieved 10 Feb 2010. from <http://webstats.3gpp.org/ftp/Specs/html-info/22968.htm>.

The Federal Communications Commission. (2005). *Review of the Emergency Alert System*. Retrieved 13 April 2008. from <http://www.fcc.gov/eb/Orders/2005/FCC-05-191A1.html>.

The International Telecommunications Union. (2007). *Compendium of ITU'S Work on Emergency Telecommunications*. Geneva, Switzerland: The United Nations Agency for Information and Communication Technologies.

The Minister for Police and Emergency Services. (2005). *First Calls Made as Part of Early Warning Trial*. Retrieved 04 June 2007. from http://www.legislation.vic.gov.au/domino/Web_Notes/newmedia.nsf/35504bc71d3adebcca256cfc0082c2b8/4ae0fe91bdeb3e8aca25704d000729b0!OpenDocument.

The United States Department of Homeland Security. (2008). *National Emergency Communications Plan*. Retrieved 06 October 2009. from http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

The Victorian Bushfires Royal Commission. (2009). *Victorian Bushfires Royal Commission Interim Report*. Retrieved 03 October 2009. from.

The Victorian Department of Treasury and Finance. (2009). *Request for Information (RFI) for: Location Based Identification of Active Mobile Handsets for Emergency Notification Purposes. RFI Number: SS-06-2009*. Retrieved 19 November 2009. from

<https://www.tenders.vic.gov.au/tenders/tender/display/tender-details.do?id=87&action=display-tender-details&returnUrl=%2Ftender%2Fsearch%2Ftender-search.do%3Faction%3Dadvanced-tender-search-closed-tender>.

- Togt, R., Beinat, E., Zlatanova, S., & Scholten, H. (2005). Location Interoperability Services for Medical Emergency Operations during Disasters. In P. v. Oosterom, S. Zlatanova & E. M. Fendel (Eds.), *Geo-information for Disaster Management* (pp. 1127-1141). Berlin Heidelberg: Springer
- Tsalgatidou, A., Veijalainen, J., Markkula, J., Katasonov, A., & Hadjiefthymiades, S. (2003). *Mobile E-Commerce and Location-Based Services: Technology and Requirements*. Paper presented at the The 9th Scandinavian Research Conference on Geographical Information Sciences, Espoo, Finland.
- Uhlirz, M. (2007). A Market and User View on LBS. In G. Gartner, W. Cartwright & M. P. Peterson (Eds.), *Location Based Services and TeleCartography* (1st ed., pp. 47-58). Berlin Heidelberg: Springer.
- United Nations News Centre. (2010). Earthquakes the deadliest of all disasters during past decade [Electronic Version]. Retrieved 29 January 2010 from <http://www.un.org/apps/news/printnews.asp?nid=33613>.
- Victorian State Parliamentary Offices. (2003). *Watching Brief on the War on Terrorism: Submission by the State Of Victoria to the Joint Standing Committee on Foreign Affairs, Defence and Trade Hearing on Australia's Counter Terrorism Capabilities*. Retrieved 18 January 2009. from <http://www.aph.gov.au/House/committee/jfadt/terrorism/subs/sub13.pdf>.

ADDITIONAL READING SECTION

- Aloudat, A., Michael, K., & Jun, Y. (2007). Location-Based Services in Emergency Management- from Government to Citizens: Global Case Studies. In P. Mendis, J. Lai, E. Dawson & H. Abbass (Eds.), *Recent Advances in Security Technology* (pp. 190-201). Melbourne: Australian Homeland Security Research Centre.
- Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (1st ed.). Boulder, Colorado: Perseus Press.
- Cantwell, B. (2002). *Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies*. Working Paper, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, Massachusetts. Retrieved 17 August 2009.
- Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal*, 15(1), 5-25.
- Code of Practice of Passive Location Services in the UK. (2006). Industry Code of Practice For the use of mobile phone technology to provide passive location services in the UK. Retrieved 23 August 2007, from http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf
- Gow, G. A. (2005). Pinpointing Consent: Location Privacy and Mobile Phones. In K. Nyíri (Ed.), *A sense of place: The global and the local in mobile communication* (pp. 139-150). Vienna: Passagen Verlag.

- Holtzman, D. H. (2006). *Privacy Lost: How Technology Is Endangering Your Privacy* (1st ed.). San Francisco, California: Jossey-Bass.
- Kiefer, J. J., Mancini, J. A., Morrow, B. H., Gladwin, H., & Stewart, T. A. (2008). *Providing Access to Resilience-Enhancing Technologies for Disadvantaged Communities and Vulnerable Populations*. Retrieved from www.orau.org/university-partnerships/files/The-PARET-Report.pdf.
- Kim, D. J., Braynov, S. B., Rao, H. R., & Song, Y. I. (2001, 2-5 August). *A B-to-C Trust Model for Online Exchange*. Paper presented at the Seventh Americas Conference on Information Systems, Boston, Massachusetts.
- Kini, A., & Choobineh, J. (1998). *Trust in Electronic Commerce: Definition and Theoretical Considerations*. Paper presented at the Thirty-First Annual Hawaii International Conference on System Sciences.
- Krishnamurthy, N. (2002). *Using SMS to deliver location-based services*. Paper presented at the 2002 IEEE International Conference on Personal Wireless Communications.
- Marx, G. T. (1999). What's in a Name? Some Reflections on the Sociology of Anonymity. [Article]. *Information Society*, 15(2), 99-112.
- McAdams, J. (2006). SMS does SOS: Short Message Service Earns Valued Role as a Link of Last Resort for Crisis Communications. Retrieved 02 February 2007, from http://fcw.com/articles/2006/04/03/sms-does-sos.aspx?sc_lang=en
- McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, 6(2), 35-59.
- Perusco, L., Michael, K., & Michael, M. G. (2006, 11-13 Oct.). *Location-Based Services and the Privacy-Security Dichotomy*. Paper presented at the Third International Conference on Mobile Computing and Ubiquitous Networking, London.
- Pura, M. (2005). Linking perceived value and loyalty in location-based mobile services. *Managing Service Quality*, 15(6), 509 - 538.
- Schneier, B. (2008). The Myth of the 'Transparent Society'. *Wired Magazine*. Retrieved from http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306
- Tan, Y.-H., & Thoen, W. (2001). Toward a Generic Model of Trust for Electronic Commerce. *International Journal of Electronic Commerce*, 5(2), 61-74.
- The Australian Communications and Media Authority. (2004). *Location Location Location: The Future Use of Location Information to Enhance the Handling of Emergency Mobile Phone Calls*. Retrieved from http://acma.gov.au/webwr/consumer_info/location.pdf.
- The Australian Government: Attorney General's Department. (2008). Privacy Act 1988: Act No.119 of 1988 as amended. Retrieved 02 August 2008, from [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/63C00ADD09B982ECCA257490002B9D57/\\$file/Privacy1988_WD02HYP.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/63C00ADD09B982ECCA257490002B9D57/$file/Privacy1988_WD02HYP.pdf)

Weiss, D., Kramer, I., Treu, G., & Kupper, A. (2006). *Zone Services - An Approach for Location-Based Data Collection*. Paper presented at the The 8th IEEE International Conference on E-Commerce Technology, The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services.

KEY TERMS & DEFINITIONS

Emergency Management: typically has four stages including prevention/mitigation, preparedness, response and recovery. Emergency management is integral to a nation's national security from the perspective of societal securitization.

Hazards: these can be natural or technological. Natural hazards are those that have their origin in the natural environment such as bushfires. Technological hazards are a result of failures in human-made systems, such as oil spills. Hazards can also be categorized as chemical, biological or radiological.

Integrated Public Number Database (IPND): an industry-wide, commonwealth-owned database that contains all the residential and business telephone numbers (listed and unlisted) of Australia. The IPND also stores subscriber information such as name, address, and the type of service delivered by each number (e.g. landline or mobile).

Information Privacy: the interest an individual has in controlling the handling of data about themselves.

Information Risk: Personal data being accessed or modified by unauthorized persons.

Location-Based Services: services that use the location of the target for adding value to the service, where the target is the "entity" to be located. Typical LBS consumer applications include roadside assistance and who is nearest, and typical LBS business applications include fleet management and field service personnel management.

Mandate: A command or an authorization given by a political electorate to its representative often supported by laws and regulations.

Mobile Alerts: A message disseminated during an emergency to mobile devices, typically sent from an authorized government agency.

Security: Freedom from risk or danger; safety. Freedom from doubt, anxiety, or fear.

Short Message Service: SMS is a well-known and accepted asynchronous protocol of communication. It is capable of transmitting a limited size of binary or text messages to one or more recipients. SMS offers virtual guarantee for message delivery to its destination.