# Chapter 7
# The Socio-Ethical Considerations Surrounding Government Mandated Location-Based Services during Emergencies:
## An Australian Case Study

**Anas Aloudat**
*University of Wollongong, Australia*

**Katina Michael**
*University of Wollongong, Australia*

## 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 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.*

## INTRODUCTION

The aim of this chapter is to present a case study on how modern technologies, namely mobile applications, are changing the landscape of emergency management in Australia. The chapter 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.

## 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

24 more pages are available in the full version of this document, which may
be purchased using the "Add to Cart" button on the publisher's webpage:
[www.igi-global.com/chapter/socio-ethical-considerations-surrounding-government/52941](www.igi-global.com/chapter/socio-ethical-considerations-surrounding-government/52941)

# Related Content

### Blockchain-Based Educational Management and Secure Software-Defined Networking in Smart Communities
Bin Fang (2022). *International Journal of Information Security and Privacy (pp. 1-20).*
[www.irma-international.org/article/blockchain-based-educational-management-and-secure-software-defined-networking-in-smart-communities/308314](www.irma-international.org/article/blockchain-based-educational-management-and-secure-software-defined-networking-in-smart-communities/308314)

### Considerations for Blockchain-Based Online Dispute Resolution
Madhvendra Singhand Nitya Jain (2022). *Handbook of Research on Cyber Law, Data Protection, and Privacy (pp. 212-230).*
[www.irma-international.org/chapter/considerations-for-blockchain-based-online-dispute-resolution/300913](www.irma-international.org/chapter/considerations-for-blockchain-based-online-dispute-resolution/300913)

### Privacy and Other Legal Concerns in the Wake of Deepfake Technology: Comparative Study of India, US, and China
Purva Kaushik (2022). *Handbook of Research on Cyber Law, Data Protection, and Privacy (pp. 37-49).*
[www.irma-international.org/chapter/privacy-and-other-legal-concerns-in-the-wake-of-deepfake-technology/300903](www.irma-international.org/chapter/privacy-and-other-legal-concerns-in-the-wake-of-deepfake-technology/300903)

### A Model to Improve Security Questions Through Individualized Assistance
Andrew Mangle, Sandip Patel, Sanjay Bapna, XingXing Zuand David Gurzick (2021). *International Journal of Information Security and Privacy (pp. 31-53).*
[www.irma-international.org/article/a-model-to-improve-security-questions-through-individualized-assistance/289819](www.irma-international.org/article/a-model-to-improve-security-questions-through-individualized-assistance/289819)

### Data Mining and Economic Crime Risk Management
Mieke Jans, Nadine Lybaertand Koen Vanhoof (2011). *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection  (pp. 205-227).*
[www.irma-international.org/chapter/data-mining-economic-crime-risk/46812](www.irma-international.org/chapter/data-mining-economic-crime-risk/46812)