2008

The social impact of national security technologies: ePassports, E911 and mobile alerts

Holly Tootell

University of Wollongong, holly@uow.edu.au

Publication Details

The social impact of national security technologies: ePassports, E911 and mobile alerts

Abstract
This paper explores the adoption of emerging technologies for the purposes of national security. The three technologies chosen were ePassports, E911 and mobile alerts. The study uses a content analysis methodology drawing on popular media documentation to extract the major social and technological impacts of the technologies on citizens as they were reported. The findings of the study indicate that reactions to the three technologies differed. ePassports were considered vastly different to E911 and mobile alerting predominantly because they were seen to be a controlling technology, whereas E911 and mobile alerting were viewed to be about safety and emergency response.

Keywords
social, impact, national, security, technologies, ePassports, E911, mobile, alerts

Disciplines
Physical Sciences and Mathematics

Publication Details
The social impact of national security technologies: ePassports, E911 and mobile alerts

Holly Tootell
Lecturer, School of Information Systems and Technology, University of Wollongong

Abstract
This paper explores the adoption of emerging technologies for the purposes of national security. The three technologies chosen were ePassports, E911 and mobile alerts. The study uses a content analysis methodology drawing on popular media documentation to extract the major social and technological impacts of the technologies on citizens as they were reported. The findings of the study indicate that reactions to the three technologies differed. ePassports were considered vastly different to E911 and mobile alerting predominantly because they were seen to be a controlling technology, whereas E911 and mobile alerting were viewed to be about safety and emergency response.

Keywords: radio-frequency identification (RFID), E911, mobile alerting, national security

1 Introduction
The purpose of this paper is to explore the coverage of three technologies being used for national security applications. The concepts of terrorism, security, privacy and liberty are factors that can be shaped by the media in respect to events of national security significance. This paper examines three technologies being used for terrorism response, natural disasters and epidemics. Location-based technologies fulfil an important role in emergency management. Emergency management involves looking at the entire spectrum of emergency needs including prevention, protection and response. In Australia, Emergency Management Australia (EMA) is the government body responsible for emergency management. It is situated in the federal Attorney-General’s Department (EMA 2006). In the US, the equivalent body is known as the Federal Emergency Management Agency (FEMA), and is part of the Department of Homeland Security. The common objective of emergency management bodies such as this is to provide a comprehensive strategy to reduce the loss of life and property and protect the respective country from all hazards,
including natural disasters, acts of terrorism, and other man-made disasters, by coordinating with all agencies in an emergency management system of preparedness, protection, response, recovery, and mitigation (FEMA 2007). Through the analysis presented in this paper, the attitudes towards three of these technologies will be explored. The technologies that have been chosen include: RFID passports (ePassports), the United States-based E911 service and mobile alerting in emergency situations.

2 Data Collection

The data used in this paper is derived from articles retrieved from a number of online databases (Proquest5000, ACM Digital Library, IEEE Explore and Factiva). Each of the databases are international, multidisciplinary databases that incorporate a wide variety of sources including academic journals, newspapers, newswires and industry publications. This variety of sources ensured that the technicalities of the concepts which are not often covered in mainstream media would be included.

Each of these databases was searched for articles relating to the deployment of each of the three technologies using the relevant terms shown in Table 1. Articles relating to the financial status of the company were included in many of the searches because of the impact that one or more national security events have had on the developer or technology partners behind the deployment.

Table 1 Technology search terms

<table>
<thead>
<tr>
<th>Technology</th>
<th>Search term</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID passports</td>
<td>(RFID passports) or (ePassport)</td>
</tr>
<tr>
<td>E911</td>
<td>E911</td>
</tr>
<tr>
<td>Mobile alerting</td>
<td>(emergency alert) and (SARS)</td>
</tr>
<tr>
<td></td>
<td>(SMS or mobile or cell) and (emergency or alert)</td>
</tr>
</tbody>
</table>

3 ePassport for National Security

The US Department of Homeland Security has pushed for a worldwide standard for enhanced machine readable passports since September 11. A part of this initiative is the proposal to include RFID chips in all passports. One of the key problems with the inclusion of an RFID chip is that the passport holder will be "continuously broadcasting their name, nationality, age, address and whatever else is on the RFID chip" (Schneider 2004). Any receiving device would be able to read the data. Proponents of the technology claim it is the most suitable technology for the task, in preference to a contact smart card, because of advantages including faster processing at customs checks and increasing the difficulty of forging or altering the document. Other countries promoting this approach include Australia and the UK, who have been encouraged by the US initiative to have compatible and conforming systems.

3.1 Data Analysis

The primary theme identified through the content analysis was technology (Table 2). In many of the articles, the potential of the ePassport technology is identified and is followed by discussion of the risks it poses (Leach 2004; Ledlow 2005). Neumann and Weinstein (2006) identify this issue in a more general context, and in a much less negative light than Leach (2004) and Ledlow (2005). The potential of the technology, described by Leach (2004) was to "create a more secure travel document". In light of this though are the opinions of those who see a potential mismatch in agenda between government, businesses and the public. Michael and Michael (2006, p.361) address this theme noting that the influence of media and government policy have significant sway on public opinion.

Table 2 ePassport themes

<table>
<thead>
<tr>
<th>Concept</th>
<th>Discussion themes</th>
</tr>
</thead>
<tbody>
<tr>
<td>technology</td>
<td>Considers the impact of the RFID chips, from their potential to impact on the public and achieve security.</td>
</tr>
<tr>
<td>data</td>
<td>The collection of information and the potential of tracking, and identification through the use of RFID chips.</td>
</tr>
<tr>
<td>risk</td>
<td>This theme represents the context (war and terrorist) within which this technology solution has been offered.</td>
</tr>
<tr>
<td>privacy</td>
<td>Privacy is of particular interest in respect to government use of information.</td>
</tr>
<tr>
<td>systems</td>
<td>This theme represents the players in this technology: business, people, and world.</td>
</tr>
<tr>
<td>chips</td>
<td>RFID-enabled passports will have a chip. In this context the idea of personal application, digital technology, and the ability to read the data are a focus.</td>
</tr>
</tbody>
</table>

The interplay between these actors (government, business and the public) is picked up in the observation that:

Consumer privacy groups have grown in strength this year almost as fast as radio frequency identification technology deployments at businesses and governments (Albrecht 2005).

Glover (2005) is steadfast in his position on the technologies being combined at the risk of obliteration of “traditional ideas of personal privacy”. This theme ties closely to surveillance of individuals. Hoversten (2004), Amoore and Goede (2005) and Archer and Salazar (2005) consider the issue of surveillance through the RFID technology being used to track consumer behaviour. With a tone of resignation, the authors believe that it will become an accepted part of life because of the pervasive requirements of the technology in its application. They also note that the practice of surveillance is enabled and made easier through the development of RFID technology. It must be noted that many still argue that RFID is not a tracking technology. Passive tags cannot be used to track, but active tags can be used for tracking purposes (O'Connon 2006).

The impact of RFID technology is being closely monitored through privacy advocacy groups (Albrecht and McIntyre 2005; Tebo 2006) who are encouraging the development and safeguard of legislation to protect consumers. Albrecht (2005) takes a strong position arguing that the current technology-centric attitudes are creating a problem for future generations in being able to define and subsequently defend the notion of privacy. What is apparent in this content analysis is that the dominant attitudes in terms of risk to privacy are negative. Technology-positive attitudes are overshadowed. In the post-September 11 climate, although there is unease for security on both a personal and a national level, the impact of proposed measures to address these security concerns is being given serious consideration.
What scares me is you have people developing RFID technology, spending hundred of millions of dollars, who are looking at the rest of us and saying, risk, there's no risk. As a result they're not taking any precautions to protect us down the road. Our children's and grandchildren's generation will look back and history will judge us based on how we handle this threat (Albrecht 2005).

It is clear from the data that privacy and security of information is paramount. In the US experience, the perceived premature deployment of RFID technology resulted in an overwhelming 98.5% of 2335 survey participants responding negatively to the idea (Hoffman 2006). Of these, 2019 respondents listed security and privacy as their top concern. The flow-on effect of this is that the government has had to validate the privacy and security concerns of civil libertarians and security experts, who claim that the government is ill-prepared to deal with the issues raised by the technology (Gonsalves 2005; Rockwell 2006). Sullivan (2005) is also concerned by the issue of premature deployment of the RFID technology because technology developers are ignoring the risks and are not incorporating sufficient concern for future impacts of the technology.

Further to the technology-based concerns is the issue of 'skimming' from distances greater than first thought possible, which presents another privacy concern (Lipton 2005). The technology perspective also raises concern regarding the heavy reliance by governments on increasingly sophisticated technology solutions (Amoore and De Goede 2005).

Arguments raised by civil libertarians often tend toward extremist or worst-case scenarios which directly contribute to the perception of risk and fear. The American Civil Liberties Union suggests that RFID readers could be used by terrorists to identify US citizens as they walk down the street (Gardner 2005). Albrecht (2005) is quite pessimistic in stating that:

> RFID could put us and our information at the mercy of global corporations and government bureaucracies and strip away the last shreds of privacy we have left.

From a national security perspective, there is strong evidence to support the swing towards more control and power in border control. Kliment (2006) puts forward that "the US has tried to use technology to balance the competing claims of border security, individual privacy and international commerce". McHale (2005), Biba (2005) and Loftus et al. (2006) bring to light the perceived dichotomy between privacy and security.

McHale (2005) quotes vice president of Civitas Group, Rick Gordon, as claiming that "it is possible to control the borders thoroughly through technology, but political considerations such as the right to privacy can get in the way". Biba (2005) weighs up the benefits of faster and more secure border entry, but at the cost of personal privacy. Soppola and Burbridge (2005) and Loftus et al. (2006) report the necessity of dealing with privacy and security concerns at the outset of the technology deployment to "reduce the costs of dealing with these later".

### Table 3 ePassport ranked list of concepts

| technology, security, chips, information, data, systems, privacy, tags, cards, government, U.S., people, personal, risk, track, read, biometric, identity, industry, company, number, digital, world, public, potential, war, terrorist, business, money, surveillance |

Table 3 is a ranked list of concepts from the content analysis. In the ranked list risk is not as prominent as the issue of privacy. Privacy has direct relationships to the data and information that is potentially collected from the systems, whereas risk is considered as a pervasive concern which is not linked to one major issue. Interestingly, the concept of surveillance is the lowest ranked term. There is no direct link between the issue of privacy and the collection of information. However, it most certainly forms part of the wider concept of the risk of the technology.

#### Diagram 1 Technology and social impact of ePassports

In Diagram 1, the concepts from Table 3 have been categorised as technology impact or social impact. In the data collected, there is a greater emphasis on the social impact of this technology. This reflects the media coverage focus on the threat and fear associated with the September 11 attacks. By focusing on the fear, the potential impact of the technology attracts less attention. With the implementation of the ePassport technology as a response to the September 11 attacks, it is expected that this technology will receive relatively little attention. Its introduction was portrayed as a necessary development to prevent a similar attack occurring.

### 4 E911 for emergency services

E911 (Enhanced 911) is a location technology supported by the US Federal Communications Commission (FCC). Prior to 1996, the service had been available to wired telephony users. The mobile equivalent enables mobile phones to process 911 emergency calls and emergency services to locate the caller's phone number and geographic position of the caller (Dawson et al. 2007, p.4). Prior to the E911 proposal, only a subscriber's carrier was able to handle the call. The new ruling meant that all 911 calls from mobile phones were to be handled by any available service provider. There were two phases to E911. The first, in 1998, required that the phone number be identified and location of the signal tower (cell) is accurate to within a mile. Phase II, in 2001, required mobile phone companies conducting business in the US to offer either handset- or network-based location detection functionality so that “two-thirds of emergency calls received require the location of the individual to be accurate to within 50 metres, and 95 per cent of calls to within 150 metres” (Michael 2004).
4.1 Data analysis

The primary themes identified in the E911 data are shown in Table 3. The concept of location is central to the E911 debate. Wireless and systems refer to the technology focus in the implementation of this scheme. Closely related to location is the issue of privacy. Minor issues raised in the source material refer to signal and state. The signal concept is related to the technology focus of wireless and systems. State refers to the role the FCC and whole government has had in the implementation of the E911 initiative.

Table 3 E911 themes

<table>
<thead>
<tr>
<th>Concept</th>
<th>Discussion</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Considers the technology in terms of determining location through signals, and bases. It also considers the impact of application and the role of phone providers.</td>
<td></td>
</tr>
<tr>
<td>wireless</td>
<td>This theme is concerned with the emergency communications process through calls and carriers.</td>
<td></td>
</tr>
<tr>
<td>privacy</td>
<td>Although a larger issue, this theme is specifically focused on privacy in relation to the companies participating in the E911 scheme.</td>
<td></td>
</tr>
<tr>
<td>systems</td>
<td>This theme brings together considerations of data and reliability.</td>
<td></td>
</tr>
<tr>
<td>signal</td>
<td>Technology focused theme centres on position, strength in relation to signals.</td>
<td></td>
</tr>
<tr>
<td>state</td>
<td>The concern of this theme is on the role of the states in effectively supporting and implementing the E911 initiative.</td>
<td></td>
</tr>
</tbody>
</table>

Much of the media coverage is optimistic regarding the use of the technology as an emergency location identification technology. Behr (2001) has identified the main concern of the technology as the potential of commercial interest in the collected information, separate from the safety uses. He goes on to report that “61 percent said they would be concerned if businesses had access to the information” (Behr 2001). The impact and probability of this is reported by Gold (2000) on mobile provider Sprint, already planning to use the “Qualcomm-supplied GPS-assisted wireless location technology for calls other than E911 ones”. Selzter (2005) identifies a different perspective on the role of the vendors using the E911 equipment for other purposes, being quick to point out that the vendors “are anxious not to get into the middle of such matters and would probably be happy to require user consent before recording and using any location data” even though this secondary use may provide a way of recompensing the expenditure to upgrade systems to comply with the mandate. Selzter (2005) succinctly describes this as “a tricky dance of convenience vs. trouble, typical of modern technology”.

The privacy concerns regarding E911 revolve around the collection and misuse of stored data. Ross (2004) observes that the government is hesitant to advocate the need for enhanced privacy in regard to the technology, suggesting that “no administration ever would because it wouldn’t want to limit its ability to obtain information”. There is a definite call for transparency in the data collection and use practices, which Ross (2004) and Smith (2006) both reflect on. Prior to the deployment of the current phases of E911, the issue of privacy in relation to the systems supporting the technology were a concern. Gram (1999) and James (1999) talk about preserving the privacy of a new computer database that links the calling phone number with names and locations. Representatives from privacy advocacy groups have been concerned with the risk of misuse of information for a number of years, including the threat that misuse could be initiated “not only by the government but also by the phone companies themselves” according to Jim Dempsey in James (1999). Maintaining a narrow focus of use of information for specific purposes is one suggested means of overcoming the threat of information misuse. Ross (2004) and Smith (2006) suggest that terrorism is one of the issues where there is a good balance between privacy and the need for law enforcement. They have also put forward that the advancement of technology has provided benefits in terms of safety monitoring and response, but has also increased vulnerabilities in relation to the collection of information.

Table 4 E911 Ranked list of concepts

<table>
<thead>
<tr>
<th>Concept</th>
<th>Discussion</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Wireless technology, information, services, systems, emergency, system, phone, E911, service, calls, carriers, mobile, data, FCC, public, provide, state, network, phones, number, cell, GPS, privacy, providers, applications, cellular, companies, industry, access, available, personal, telephone, people, base, communications, signal, meet, position, research, area, infrastructure, case.</td>
<td></td>
</tr>
</tbody>
</table>

The ranking of privacy is interesting to note in Table 4. It is of less concern in the E911 than the ePassport data collection. There is an implication in the reporting of this technology that it is less invasive and pervasive than the ePassport initiative. This may be due to the fact that the E911 service is a pull technology, where users are asking for help. In situations where the E911 service is likely to be requested, the user will be in need of assistance, and not in a position to be too concerned about the implications of the technology.

Diagram 2 Technology and social impact of E911

The division between the technology impact and social impact concepts related to E911 (Diagram 2) is more heavily weighted toward the technology than the ePassport initiative division of concepts. More descriptive information about the technology is common in the E911 coverage. As the E911 initiative was developed, it was openly discussed in the newspapers and government, which may account for the greater focus. The overlap in Diagram 2 illustrates the blending of the technology issues and social issues, and is indicative of the interaction between the social impact and the technology development.
5 Mobile Alerting for Commercial Application Based on SARS Outbreak

Mobile alerting allows users of mobile phones to receive messages regarding location-specific information. For everyday use, mobile alerting is a subscription-based service packaged as an add-on to the ordinary payment plan. During the SARS outbreak, Hong Kong mobile phone provider Sunday Telecom, and Singapore-based provider Starhub had an opt-in service in which subscribers had their phones tracked (Michael and Masters 2006). When the mobile phone came within a one kilometre radius of a reported SARS case, an SMS would be sent to notify of the affected building (Staff 2003). This service can be used for many applications; emergency communications is one example, others include: find a friend services, and location specific restaurant and shopping offers.

5.1 Data Analysis

The primary themes identified in the Mobile Alerting data are shown and described in Table 5. The relationship of these terms provides the structure for the following discussion.

Table 5 Mobile alerting themes

<table>
<thead>
<tr>
<th>Concept</th>
<th>Discussion issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>people</td>
<td>This theme represents the impact that the SARS outbreak has had on the world. It includes information regarding the spread of the disease.</td>
</tr>
<tr>
<td>mobile</td>
<td>The role of companies, services and subscribers is covered in this theme.</td>
</tr>
<tr>
<td>services</td>
<td>This concept represents the SMS alerts from a network and patient perspective.</td>
</tr>
<tr>
<td>system</td>
<td>It is important to recognise the role of the public health system in managing the global outbreak.</td>
</tr>
<tr>
<td>technology</td>
<td>This theme identifies the development of the early warning emergency notification systems.</td>
</tr>
</tbody>
</table>

Mobile alerting technology brings many benefits in emergency alert applications, but a number of issues, including privacy and network infrastructure, are viewed as impediments to fast and complete deployment (Christopher 2006). From a user's perspective, any potential downside to the subscription service is outweighed by the benefits of the location-based warnings, especially those needing to work in affected areas (Wong 2003). The immediate threat of SARS contributed to the popularity of the mobile alerting service. The ease of signing up for the alerts (Lui 2003) and the perceived benefits they delivered meant that the mobile alerting was extremely convenient for users. The convenience of the mobile alerting is also greater than the newspaper service as noted by Wong (2003).

Wickham (2005) identifies a number of logistical considerations of releasing "all-points bulletin for all devices across all carriers within a specific geography." He believes it is an opportunity for government and business to come together to create a workable plan for meeting all requirements addressing the needs of everyone from emergency service providers to customers.

Sunday Communications launched the location-based SARS alert service in Hong Kong. It was designed to alert subscribers when they were within one mile of a building where people have been infected by SARS (Liu 2003; Lui 2003; Ramakrishnan 2003; Spy Blog 2005). From the success of this alerting system, Sunday Communications has gone on to provide other location-based notifications.

The success and acceptance of the SARS mobile alert model has impacted in various areas. Eysenbach (2003) expands the notion, illustrating the idea with remote patient monitoring systems that can be adapted to early warning systems for widespread outbreaks of infectious diseases.

The financial impact of SARS was felt strongly by mobile providers. The decline in roaming revenue due to reduced travel was countered by the increase in call traffic. It was noted that telephone communication was preferred to face-to-face contact during the initial period (Yuk-min 2003; Zuckerman 2003).

Table 6 Mobile alerting ranked list of concepts

Hong Kong, mobile, people, phone, service, outbreak, system, health, disease, phones, information, world, company, million, government, services, spread, local, SMS, global, public, patients, subscribers, countries, alert, technology, early, reserved, network, emergency

Table 6 is a ranked list of concepts from the content analysis. The focus of these terms is the impact of the technology on people. There is continued emphasis on the impact of the disease outbreak, rather than the specification of the technology. Emergency is the lowest ranked concept. The list of terms shows beyond the initial shock and emergency status of the SARS epidemic to the ongoing influence it has had on the population it affected. A number of terms refer to the international impact of mobile alerting: people, world, global, and countries.

Diagram 3 Technology and social impact of mobile alerting

The division between technology impact and social impact concepts related to mobile alerting (Diagram 3) is more heavily weighted toward the social impact than the E911 initiative. This social impact focus aligns with the results of the analysis, which determined a concentration on finding methods to manage the severity of the outbreak and communicating effectively with the population. The effect on health services is reflected strongly in Diagram 3.
6 Reflections on the media coverage of the technology

The technologies examined in this chapter were all created or further developed as a response to a national security event and in many instances, the probability of the same events occurring is minimal, but technology-based solutions were implemented regardless. There is an interesting distinction between the reactions to ePassports, E911 and mobile alerting. E911 and mobile alerting were extensions of existing technologies, where the current development and deployments were a small step from previous use, whereas the ePassport was a new development.

Table 7 News content in the mass media

<table>
<thead>
<tr>
<th>News Making</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event-driven</td>
<td>The hard core of media content. Events which actually occur and which are reported in a relatively straight-forward way.</td>
</tr>
<tr>
<td>Managed</td>
<td>These are 'created' news events, whether for commercial, political or governmental interests.</td>
</tr>
<tr>
<td>Media-coloured</td>
<td>News treatments through which events are magnified, distorted or sometimes even invented; moral panics.</td>
</tr>
</tbody>
</table>

In relation to the technologies covered in this paper, a subset of categories has been defined in Table 7. These categories will shape the discussion in the following sections.

6.1 The media response to mobile alerting and E911

The ‘selling’ points for E911 and mobile alerting appealed to the masses due to the likelihood of necessity. Mobile alerting is of particular interest in this respect, because this style of communication has become widely accepted in areas other than emergency response. As it does not require subscribers to change already adopted methods of communication, technology is not an adoption inhibitor. Both E911 and mobile alerting can be considered pull technologies. From this perspective, it is the user who instigates the use of the technology. When this is the case, there is a need perceived by the user to have that service activated. The availability of the technology and its potential impact on privacy and liberty might still be debated in theory, but at the time of need, basic survival instinct is likely to override these concerns.

The concept of privacy, in relation to mobile alerting, was not listed. This does not rule out privacy as a concern, but it does indicate that privacy concerns are low. The low level of concern may be accounted for by the pre-existing relationships between mobile phone users and the mobile networks providers, and related to the description of a pull technology above.

E911 recorded the second-most significant reaction in relation to technology acceptance. The E911 technology was a second phase of development of an existing technology. The September 11 attacks prompted further development of this service, especially in light of the confusion of the emergency response effort. Media reaction to this technology was more explanatory than confrontational in comparison to ePassport. The everyday nature of the technology meant that users did not have to adopt any additional devices or learn any new methods of operation. The invisible integration of E911 into the lives of the American people helped to create interest in the technology without it being considered an intrusion.

In terms of the styles of news making (Table 7), the coverage of both E911 and mobile alerting was predominantly event-driven. A comparison of the discussion themes for both these technologies illustrates this (see Table 8).

<table>
<thead>
<tr>
<th>9a E911 Concepts</th>
<th>Mobile Alerting Concepts</th>
<th>9b ePassport Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>people</td>
<td>technology</td>
</tr>
<tr>
<td>wireless</td>
<td>mobile</td>
<td>data</td>
</tr>
<tr>
<td>privacy</td>
<td>services</td>
<td>risk</td>
</tr>
<tr>
<td>systems</td>
<td>system</td>
<td>privacy</td>
</tr>
<tr>
<td>signal</td>
<td>technology</td>
<td>systems</td>
</tr>
<tr>
<td>state</td>
<td></td>
<td>chips</td>
</tr>
</tbody>
</table>

The terms listed in Table 8a have more to do with the actors and the components of the technology than the ePassport concepts. Although privacy rates as a concern with regard to E911, the context of it was about company use of information. The context was removed from significant personal concern and can be seen as an argument of concern about company ethics.

6.2 The Media and ePassports

The ePassport initiative was developed as a response to the September 11 attacks. It promised increased security to the holders, but also prompted curiosity as to the effectiveness of it as a preventive measure in the fight against terror. The media coverage of the technology drew on the climate of fear that prevailed in the months following the attack: which classified the coverage as managed and/or media-coloured. The questioning in the media about privacy, surveillance and tracking played a part in maintaining the 'war on terror' rhetoric. This rhetoric is now beginning to haunt the government.

Unlike the other two technologies, the ePassport is a push technology. The ePassport initiative questioned the intention of the government in relation to its citizens through the media. Consent was not sought from citizens in the US, or countries who have adopted this technology as a standard in order to comply with the US. As a push technology, the ePassport technology required travellers to take additional and different action to their normal course. Push technologies are likely to encounter resistance to adoption because of this. It is the combination of the push technology with the portrayal in the media, through managed stories and media-colouring that contributes to the different perception of the technology by the public.

The concepts identified in Table 8b mostly centre around the application of the technology and its potential for misuse. The term technology, in relation to ePassport, had connotations of mistrust between the public and government. This is different to its use in the mobile alerting context. Each of the ePassport concepts has been tempered by degrees of media-colouring, especially in regard to the creation of moral panic. Marshall and Kingsbury (1996, p.43) refer to Stanley Cohen's (1973, p.9) definition of the term 'moral panic' as:

A condition, episode, person or group of persons (that) emerges to become defined as a threat to societal values and interests; its nature is presented in a stylised and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people...

Given this definition, the context of the adoption of this technology involved more risk
than the other two examples, and tended to include coverage that had more bias toward personal and social impact rather than technology-driven concern. It is important to note that the ePassport does not act in a direct life-saving way as E911 does. This is a technology that provides protection to other travellers ‘just’ in case you are doing something wrong.

7 Conclusion

The purpose of this paper was to describe the media coverage of three technology applications being used for national security purposes. Each technology was described, and then analysed through the identified concepts. By illustrating the identified concepts in the concept map and the ranked list of concepts, connections could be made with regard to the impact of the technology deployment.

The media can act from many perspectives. The main perspectives identified in this data include the event-driven and media-coloured coverage. These categories help to describe and understand the findings that show the balance between social impact and technology impact. The use of media coverage in this paper to gauge reactions to the technologies has continued to shape the perceptions of interest: privacy, security and liberty.

References

Albrecht, K. & McIntyre, L. 2005, Spychips: how major corporations and government plan to track your every move with RFID, Nelsen Current, Nashville.
Cohen, S. 1973, Folk Devils and Moral Panics, Paladin, St Albans.
Gardner, W.D. 2005, ‘E-Passport program rolls out in Singapore’, InformationWeek, vol. April 11,