# Privacy of a mobile phone user in a rapidly evolving technological framework

Richard Syme #S9908632
School of Mathematical and Geospatial Sciences
RMIT University, Melbourne, Australia.
richard.syme@yahoo.com.au

**Key terms:**

Mobile phone
Privacy
Wireless
Network
LBS
GPS
RFID

**Abstract**

The rapid development of positioning technology and wireless networks has meant that a mobile phone has become an extremely versatile and powerful device. A contemporary mobile phone can make video calls, record and share multimedia, send and receive emails, surf the Internet and take advantage of Global Positioning System (GPS) technology to access Location Based Services (LBS). The combination of these technologies into a compact, stylish and portable device has led to a phenomenal and unprecedented number of mobile phone users. To many of these users, the use of a Location Based Service does not constitute a loss of privacy. Typically a user is not aware of what information they are divulging and where this information is stored. It is important to inform users what information they might be sharing so they can make informed decisions on how their location information is used and handled.

## Contents

## Introduction

Location data is very powerful data. In the wrong hands, location data can be used to build up an extremely intimate profile of a mobile phone user. This profile can be created from simple phone traffic data such as time, place and length of a call, to more intrusive location information such as the precise location of a user in real time using GPS or network based tracking. There would have to be a strong motive for building up this profile but access to this data must be controlled and regulated by the necessary authorities to ensure privacy of innocent mobile phone users.

This paper outlines how location data created by mobile phones can be used to track a mobile phone user. A selection of location data applications are presented to give an insight into the wide scope and contemporary use of location information. The processes behind typical location data transactions are detailed and the implications on privacy are given with a preferred privacy option identified. Finally, privacy concerns are discussed and recommendations given on how future privacy policy can be developed in relation to location data.

## Telecommunications and privacy

Users of mobile phones are divulging increasingly more information about their location and behaviour based on location data created when using their mobile phone; from simple activities such as making a phone call to more advanced requests such as accessing Location Based Services (LBS). Location information can be in the form of telecommunications traffic data collected for billing purposes or precise location data which records the user's position on the Earth's surface.

Telecommunications traffic data is data that is collected to facilitate billing purposes. Traffic data in mobile phones is not a new concept, as traditional fixed line billing requires the same traffic data to be collected. Penders (2004) explains that traffic data are generated to direct the communications. Types of traffic data collected include the calling number, the dialled number and the time the call started and finished. What is not recorded is the communication itself i.e. the voice conversation (Penders, 2004). Traffic data can be considered sensitive information as it can be ascertained who is calling who and at what time. By looking at the data over time and the length of each call, behavioural patterns can be identified and personal information can be inferred about the mobile phone user. For example, a one-off phone call during business hours may indicate a professional and business-like relationship between caller and receiver. On the other hand, repeated long phone calls late at night might indicate a more personal relationship. This information can be considered private and should be collected only to facilitate the provision of the service. Furthermore, access to this data should be restricted to those who only require it for the purposes of billing.

## Mobile phone positioning technology

There are two methods of determining the location of a mobile phone or user:

1) The network-based method which is calculated by the telecommunication service provider independently from the user; and

2) The handset-based method which requires input from the mobile phone user and utilises positioning technology built into the mobile phone.

**Network-based method**

In a cellular network, a mobile phone is wirelessly connected to a base station (transmission tower). Penders (2004) explains that while in the service area of this base station, the user can wander around freely while still maintaining the radio-link with the base station. To physically connect the user to another mobile phone user, the telecommunication service provider must know which base station the user is wirelessly connected. The area that a transmission tower services is known as the cell, and varies in size. Knowing the location and size of the cell, the user's location can be pinpointed at best to 500 metres and at worst to a couple of kilometres (CapGemini, 2005). One of the disadvantages with the network-based positioning method is that the accuracy of this position is limited to the size of the base station service area (cell size) and worsens considerably as the user moves into rural areas as cell sizes are much larger (Gadzheva, 2007). This method of locating a mobile phone, known as Cell-ID, is the most common method of mobile phone tracking in urban areas. Another method, known as Enhanced Cell-ID uses additional information such as Time of Arrival (TOA) and Observed Time Difference (OTD) to try and derive a more accurate position (Gadzheva, 2008).

**Handset-based (GPS) method**

The second method of locating a mobile phone user consists of using positioning technology built into the user's device. This method makes use of the phones inbuilt Global Positioning System (GPS) chipset (CapGemini, 2005). To be able to locate the mobile phone using GPS, a signal from the phone must first be sent. The disadvantage with the GPS method is that if lines of sight cannot be made with satellites, a position cannot be determined. In rural and open areas GPS works well but in cities or inside buildings where the satellite view is blocked by buildings, the user's position cannot be determined (Gadzheva, 2008). It is important to note that on one hand there is a system that works well in urban areas and not in rural areas (the network-based method) and conversely there is a system that can be unreliable in urban areas and highly accurate in rural areas (GPS or handset-based method). In response to this, a combined technology known as A-GPS has been developed which makes use of the telecommunication network to locate the phone when the GPS signal is weak (CapGemini, 2005). The table below shows expected accuracy and quality of network-based and handset-based tracking methods:

| Technology | Indoor | | Urban | | Suburban | | Rural | |
|---|---|---|---|---|---|---|---|---|
| | Accuracy | Yield* | Accuracy | Yield | Accuracy | Yield | Accuracy | Yield |
| A-GPS | 200m | Low | 150m | Low | 40m | Medium | 30m | High |
| Enhanced Cell ID | 50-550m | High | 50-550m | High | 250m-2.5km | High | 250m-8km | High |
| Cell ID | 250m | High | 250m | High | <500m | High | >1000m | High |

**Figure 1 Positioning technology accuracy Source: CapGemini 2005 pp.14**

*Yield denotes a successful location attempt.

**Wireless positioning technology**

In addition to positioning a user in the world using a mobile phone, user privacy is an issue where any type of wireless surveillance is used. Wireless 'bugs' can be used to determine when an object or person is in a particular area. These 'bugs', usually small devices implanted or located on an object, are wirelessly sensed by a receiver that has a known location within the world. In this way, the location of a user can be ascertained. A typical example of this technology is given below.

**Radio Frequency Identification (RFID) tags**

There are two types of RFID tags. Passive RFID tags have no power source and have a sensing range of around a metre. Active RFID tags which have their own power source can transmit up to one 1.6km (Hayles, 2007). RFID tags are cheap and simple and can be as small as a grain of rice. RFID tags are useful for surveillance and monitoring and can transmit personal data, depending on what is stored on the tag. Due to the nature of the technology RFID tags reveal the location of a user or an object. A simple example of an RFID tag is the use of electronic tags on clothing garments in retail stores. When the item moves outside the store, sensors installed at the entry will sound an alarm, signalling a garment has left the store. When RFID tag data is linked with credit card payment data, customers can be profiled in regard to their shopping patterns (Lam 2005). Use of this location data has to be carefully controlled to protect certain users of the technology. Further examples of the use of RFID tags are given below.

**Applications of positioning technology**

There is almost endless potential in the number of applications that can be developed based on the location of a mobile phone. The most common applications are called Location Based Services (LBS). Gartner (pp. 51, 2007) explains that "a system can be called a Location Based Service (LBS), when the position of a mobile device – and therefore the position of the user – is somehow part of an information system". The possibilities for LBS are in some ways only limited by the imagination as spatial information is related to almost every aspect of life. In the next section of the paper, the wide scope and use of location information is apparent where examples of current and potential future LBS are given.

**Standard LBS**

Common LBS functions include finding the closest Point of Interest (ATM, restaurant etc), to navigational aids (quickest route, shortest distance functions) and Geo-coding (to find addresses and use addresses to plot routes). These are traditional LBS functions that millions of people use on a day-to-day basis, both on their mobile phones and on desktop computers.

**Emergencies**

There is a federal regulation in the United States that requires explicitly for all wireless carriers to provide latitude and longitude coordinates of 911 (emergency assistance) calls, pinpointing callers to a location within 50-100m (FCC, 2009). This accuracy is achieved through the sale of mobile phones with mandatory installation of a GPS chipset (Zhang, 2009).

**Law enforcement**

Ankle cuff devices are already used by the United States Justice Department on prisoners. If the prisoner should somehow escape, an alarm will be triggered. A similar device can be installed on ex-convicts on parole. If they should move outside a certain area (if this is a stipulation of their parole conditions) then an alarm will go off, alerting the authorities. RFID tags can be attached or inserted into dangerous criminals to keep an eye on them and deter them from committing further crimes. GPS is being trialled as a way of tracking convicted paedophiles and violent offenders, alerting police if they violate their parole by entering forbidden areas such as playgrounds or schoolyards (Graham-Rowe 2005).

**Child tracking**

Child tracking has already been taken up on a large scale in some countries. In Japan, children have RFID tags located on them and when they move outside their play area, an alarm goes off. This could potentially be useful in the home or around water hazards. If the child wanders outside or close to a swimming pool, an alarm will go off perhaps saving the child's life.

It is quite common for parents to supply their children with mobile phones should they need to contact them in an emergency. With the advent of positioning devices in phones, there is the potential for parents to keep track of their kids by giving them with a phone that has already been set up to be tracked. This is a contentious issue as it involves people being tracked without their knowledge or consent. It is argued that this violates civil liberties which go against the law in many countries. If mobile phone tracking is to be implemented on a large scale, these types of issues will need to be addressed.

**Vehicle tracking**

Pay as you go road charges - This use of telematic technology in vehicle tracking aims to lower road congestion and charge the users who contribute more to road congestion as opposed to all road users. This will lead to smarter use of the road system. There is a recommendation in Australia that vehicles be forced to carry a tracking device so they can be charged extra for driving on main roads and in peak hour. "The devices – similar to those used in truck fleets – would feed information to a database that would then levy charges, which would vary according to vehicle type, the road being use and the time of day" (Sharp, 2009).

Fleet and asset management - A fleet of vehicles equipped with network-based or handset-based tracking technology allows managers to find the most efficient route to destinations, check on progress of deliveries and coordinate vehicles to optimise time and reduce fuel use. Froomkin (2000) points out that "Intelligent Transport Systems" (ITS) are being implemented to manage traffic flow and prevent speeding and promise continuous, real-time information to the location of all moving vehicles.

Motorist in distress - In the situation where a motorist has broken down in their car and are lost, tracking technology can be utilised to more efficiently locate the motorist and send assistance. Using the location from the user's phone, the dispatcher can send the tow truck to the exact spot location, saving the motorist and the tow truck company valuable time.

Taxi despatching - Taxi companies in London can track the location of a caller and then dispatch the taxi exactly to their position quickly and accurately. This dramatically improves efficiency of the service and profitability of the taxi company.

**Location data custodians**

In the past, take-up of LBS has been somewhat hampered by user concerns over privacy issues (CapGemini, 2005). There is still a lot of confusion surrounding location-aware technologies and who has control over raw location data and who computes the location: the user's device, the network provider, or possibly a third party (Gadzheva, 2008). As explained earlier when it comes to positioning a mobile phone, a network-based (Cell ID or Enhanced Cell ID) or handset-based (GPS)

method can be used. Penders (2004) explains that there are several different scenarios in the transaction of location data which afford a user varying levels of privacy.

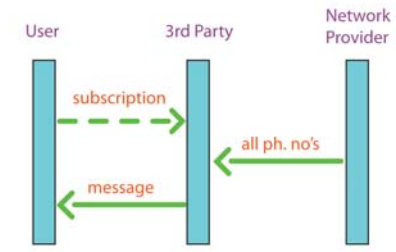
There are three parties involved in nearly all LBS request instances: the mobile phone user, the telecommunications provider and a third party. The third party provides the end-service such as location of nearest restaurants, or an SMS message from a service that the mobile user has subscribed. The user is the person who is receiving the service and the telecommunications provider is responsible for providing the location of the mobile phone. Depending on the scenario, the 3rd party will have access to varying degrees of location data, as outlined below.

**Push scenarios**

In a push scenario the 3rd party initiates contact and sends a message to a mobile phone user. For this to occur, the user must have already supplied their number to the 3rd party and given consent to receive messages. Push scenarios usually come in the form of commercial advertising and have the likely advantage of being free of charge to the user.

In a **push** scenario, there are three privacy options identified (Penders, 2004) that afford a user varying levels of privacy:

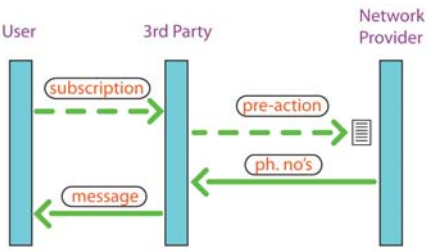
- Scenario 1 – The network provider sends the phone number of all terminals that satisfy the geographical conditions to the third party (and who have subscribed to the service). The 3rd party selects those that have applied to their service and sends them a message.




Push Scenario 1 (worst privacy)

Adapted from Penders, 2004

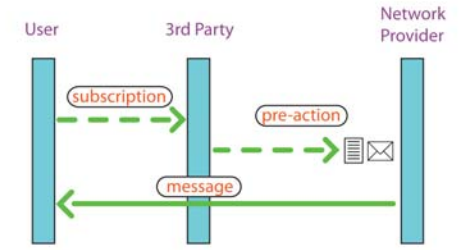
- Scenario 2 – The 3rd party has previously notified the network provider of the users which have subscribed to the service. When the 3rd party wants to send a message, the network provider checks to see which phone numbers satisfy the geographical conditions and sends these phone numbers to the 3rd party, who then sends the message.




Push Scenario 2 (moderate privacy)

Adapted from Penders, 2004

- Scenario 3 - As in design 2, the 3rd party has supplied the network provider with numbers of the subscribed users. They have also supplied the network provider with the message that they want to send. When the 3rd party wants to send the message, they notify the network provider who has all the information they need to send subscribers who match the geographic conditions the message.




Push Scenario 3 (best privacy)

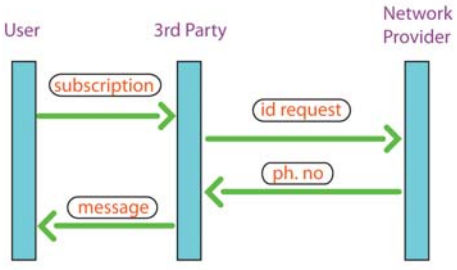
Adapted from Penders, 2004

In terms of privacy, the 3rd design is more desirable. In this design, the 3rd party never obtains phone numbers of users, therefore does not know their location. If the 3rd party does not have the location data to begin with, there is no chance that they can misuse the data or pass it on. Scenario 1 is the worst in terms of privacy as all users' phone numbers (not just subscribers) who are in the area are sent to the 3rd party. Design 2 is improved over design 1 in that only subscriber's phone numbers are sent to them. It is preferable for user location data to be handled by the network provider as they have experience dealing with private information that are bound by strict government and privacy codes of practice, therefore reducing the risk of location data ending up in the wrong hands.

**Pull scenarios**

In a **pull** scenario, a user initiates the request and in doing so gives consent. There are two possible pull scenarios, as suggested by Penders (2004):

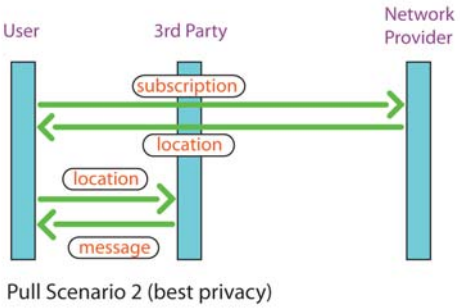
1) Scenario 1 – First, the user contacts a 3rd party with a request for a service (such as LBS). The 3rd party forwards a request to the network provider for location data, who returns the data to the 3rd party. The 3rd party uses the location data to complete the user's request.




Pull Scenario 1 (less privacy)

Adapted from Penders, 2004

2) Scenario 2 – In this scenario, the user contacts their network operator and requests their location data, which the network provider returns. Independently, the user contacts the 3rd party for a request for service and transfers his location data.



Pull Scenario 2 (best privacy)

Adapted from Penders, 2004

Pull Scenario 2 (above) is the desired choice in terms of privacy as the user has total control over their location data and when this data is accessed.

These scenarios have outlined what goes on behind the scenes when a user requests LBS. The user has several options to restrict the distribution of their location data, therefore improving their level of privacy. Of course how the network provider and 3rd party store and handle the user's location data will determine the level of privacy provided to the mobile phone user.

**Privacy concerns**

In the current age of ubiquitous computing, where multiple service providers are involved in single location data transactions, a mobile phone user could be justified in their concern for where their location data was headed and how it is handled at its destination. Penders (2004) explains that within these open networks privacy sensitive data are generated and have to be exchanged between growing numbers of parties. Gadzheva (2008) points out RFID tags, sensors and mobile phones all generate personal data and make the possibility of tracking users a reality.

In the case of a criminal investigation, it is common for law enforcement organisations to have access to location data to help solve crime. This underlines how revealing traffic communication data can be in identifying individuals and patterns of behaviour. However there is some evidence to suggest that the technology is being abused. In 2005 in the United States, the Department of Justice obtained secret permission from a judge to track a suspect without probable cause (Reilly, 2007). Their argument was that they needed to 'build a case' but the suspect was never given proper due process as stipulated by the law in that country. Examples like this do nothing to give mobile phone users confidence in the use of their location information.

When it comes to the use of mobile technology some 3rd party service providers have attempted to cover the issue of user privacy. Google (2009a) in their Mobile Privacy Policy, state that when using location-enabled services, the user might be sending actual location data (GPS data) or partial location data. The issue of how this data is handled is not addressed. Google has detailed privacy policy when it comes to non-location (web-generated) data. One would hope that location data is treated in much the same way, yet this is not implied. If Google addressed the issues of location-data privacy in their Mobile Privacy Policy it would go a long way to reassuring users that their location data is handled with the same privacy as other Google Internet traffic data.

A new Google service, called Google 'Latitude' allows friends and contacts to track one another, provided that the tracked has first permitted the tracker to do so. The technology uses both GPS chip and network based tracking technology to broadcast live a person's location on Google's website (Prigg, 2009). Human rights watchdog Privacy International claims the service is open to abuse. It says employers could supply staff with phones already set up to use the service without their knowledge, or that users could simply sign up their partner's or child's mobile phone without telling them. There is some information available as to how Google handles this location information. In Google's Latitude Tutorial Video (Google 2009b), Google informs us that only the most recent location update or manual update is stored on their servers. In other words, only the last known location of a user is recorded rather than multiple locations that can be used to build up a timeline of movement. This makes sense as Google would have no technical reason to retain historical location data and if they did it would considerably add to storage space needed on their servers.

We divulge personal information everyday to a range of professionals: our doctor, the pharmacist, an accountant or a travel agent. These different parties all have their own privacy policies that restrict the use of personal data outside of their organisation. It is where technologies overlap that personal data is exchanged between parties. The more often personal data is exchanged and the more copies of user personal data that reside in different databases, the greater chance the data could be misused or passed onto individuals or organisations that have a strong desire to access this information. Penders (2004), explains that confidentiality must be maintained in this new era where the exchange of personal data has become a prerequisite to enabling services.

In their studies on the Social Positioning Method (SPM), Ahas and Mark (2005) study social behaviour by tracking people using mobile phone technology. They report that one of the key issues in obtaining this sort of data has been people's concern for carrying a tracking device at the expense of their privacy. They suggest that this type of research will become easier to undertake as younger generations are more accepting to the possibilities of monitoring and are willing to trade their privacy to obtain a useful service. This can perhaps be supported by the fact that many of the younger generation host open social networking sites on the Internet, where a vast range of personal information such as names, birthdays, interests, hobbies and photos are shared not just between their contacts, but anyone in the world who chooses to access the site.

**Standards and regulations**

There is confusion on how to apply privacy policies to location-aware technology evident in mobile phones. There are two obvious reasons for lack of privacy policy. The rate of technological change has been so quick that policy makers have not had a chance to implement detailed privacy policy. In other words, technology has developed much faster than privacy policies and standards can be put in place. The other reason is that the technology is hard to define; there are existing privacy policies regarding telecommunications companies, computer companies and service providers, but what happens when all these technologies come together very quickly at the same time? Which policies do you implement?

This paper has shown to facilitate a single LBS request, two or more service providers are required to exchange user data. In the future, service providers must cooperate to ensure the maximum protection of user location data, which will not always be easy. As Gadzheva (2007) puts it, to ensure user trust in the service, consistent privacy standards will need to implemented across the industry and applied in practice. Governments and professional bodies must work hard to define privacy policy as it relates to user location data and then implement these policies consistently over time.

**Future developments**

In the United States privacy advocates are already working together to create a uniform policy for what carriers should do with the information they collect (Charny 2002). This includes requiring network providers telling subscribers that their location can be tracked and what plans, if any, they have for the information. This transparency would give the consumer the ultimate knowledge of what information they are divulging to whom, allowing them to make an informed decision.

It is anticipated that the technology behind much of the location-aware technology that is seen today will continue to develop at a rapid pace. As described earlier, Ahas and Mark hope that user concern over privacy problems will recede and that more people will take up tracking devices in order for them to benefit from location aware technology. Gadzheva (2007) suggests that in a future ubiquitous society, the average user will own thousands of mobile and embedded computing devices which will provide services based on the location of the user and their environment. Gadzheva (2008, pp. 452) sums it up succinctly: "The question is how to ensure the integrity and privacy of our data in untrusted ubiquitous environments and empower people with choice and informed consent, let individuals share personal information with the right people and services, in the right situations, and the right level of detail in an 'always on' wireless connectivity".

**Conclusions**

This paper has outlined the different types of technology that enable a mobile phone to be tracked. The processes behind the scenes of a LBS transaction have been revealed, showing how and when a mobile phone user's personal data is exchanged between external parties. In many LBS that people take for granted, location data is transferred between at least two parties; the network service provider and a 3rd party service provider. The data transaction scenario that restricts access to the 3rd party service provider will be the scenario which affords the user the best privacy protection.

The many benefits of LBS and location-aware technology can be demonstrated by the huge take up of mobile phones equipped with this technology. To ensure user confidence it is important to inform mobile phone users of personal data they are divulging that enables the provision of services so they can make informed decisions about their privacy. As consumers, it is important that users have consent over the release of their personal data to coincide with privacy laws found commonly in other realms of society. This will be achieved through definition and clarification of standards which can be implemented in practice and regulated across the industry.

**References**

Ahas R and Mark U (2005), 'Location based services - new challenges for planning and public administration?', *Futures 37*, no. 6, (August 1): 547-561. <http://www.proquest.com.ezproxy.lib.rmit.edu.au/> (accessed September 7, 2009)

Capgemini (2005), 'The Location-Based Services Renaissance: A New Formula for Success', *CapGemini*, viewed September 3 2009. <http://www.us.capgemini.com/DownloadLIbrary/requestfile.asp?ID=452>

Charny B (2002), 'Cell phone tracking raises privacy issues', *CNET news online*, February 27 2002, viewed September 7 2009.

FFC (2009), '9-1-1 Service', Federal Communications Commission, viewed September 10, 2009 <http://www.fcc.gov/pshs/services/911-services/>

Froomkin M (2000), 'The Death of Privacy?', *Stanford Law Review*, vol. 52, no. 5, Symposium: 'Cyberspace and Privacy: A New Legal Paradigm?', May 2000, pp. 1461-1543. <http://www.jstor.org/stable/1229519> (Accessed September 7 2009).

Gadzheva M (2007), 'Privacy concerns pertaining to location-based services', *Int. J. Intercultural Information Management*, vol. 1, No. 1, pp. 49-57.

Gadzheva M (2008), 'Location privacy in a ubiquitous computing society', *Int. J. Electronic Business*, vol. 6, No. 5, pp. 450-461.

Gartner, G (ed.) (2007), 'Development of Multimedia – Mobile and Ubiquitous', in *Multimedia Cartography*, Springer-Verlag, Berlin, pp 51 – 62.

Google (2009a), Google Mobile Privacy Policy, viewed September 7 2009. < http://www.google.com/mobile/privacy.html>

Google (2009b), "Latitude Tutorial Video", viewed September 20 2009. < http://www.google.com/privacy.html>

Graham-Rowe D (2005), 'The power to follow your every move', *NewScientist*, 16 July, viewed 23 August 2009, Nova.

Hayles K (2007), 'Ubiquitous Surveillance', Interview conducted by Gane, N, Venn, C and Hand, M, University of Tokyo, July 16 2007.

Lam T (2005), 'Technological Ubiquity: The Need for Consumer Privacy Protection', paper presented at ITU Workshop on Ubiquitous Network Societies, April 6-8 2005, Geneva. <http://www.pco.org.ht/english/files/infocentre/speech_20050407.pdf> in proceedings.

Penders J (2004), 'Privacy in (mobile) Telecommunications Services', *Ethics and Information Technology 6*, no. 4, (December 1), pp. 247. <http://www.proquest.com.ezproxy.lib.rmit.edu.au> (accessed September 7, 2009).

Prigg M (2009), 'Google phone tracker puts privacy in danger, say MPs', *Evening Standard*, March 9 2009. <http://www.proquest.com.ezproxy.lib.rmit.edu.au> (accessed September 7, 2009)

Reilly M (2007), 'We know where you are, your cellphone told us', *New Scientist*, 195(2611), pp. 24-25. Retrieved August 23, 2009, from Research Library. (Document ID: 1312212451).

Sharp A (2009), 'Vehicles forced to carry a tracking device', *Sydney Morning Herald (online)*, viewed August 14, 2009, <http://www.smh.com.au/digital-life/cartech/vehicles-forced-to-carry-a-tracking-device-20090813-ejyh.html>

Zhang K (2009), Personal communication with Dr Kefei Zhang, Associate Professor in GPS/Geodesy at RMIT University, October 9, 2009, RMIT University, Melbourne.