AN ANALYSIS OF THE RELATIONSHIP BETWEEN INDIVIDUALS' PERCEPTIONS OF PRIVACY AND MOBILE PHONE LOCATION DATA: A GROUNDED THEORY STUDY

ANDREA GORRA

A thesis submitted in partial fulfilment of the
requirements of Leeds Metropolitan University
for the degree of Doctor of Philosophy

April 2007

Abstract

The mobile phone is a ubiquitous tool in today's society, a daily companion for the majority of British citizens. The ability to trace a mobile phone's geographic position at all times via mobile phone networks generates potentially sensitive data that can be stored and shared for significant lengths of time, particularly for the purpose of crime and terrorism investigations. This thesis examines the implications of the storage and use of mobile phone location data on individuals' perceptions of privacy. The grounded theory methodology has been used to illustrate patterns and themes that are useful in understanding the broader discourses concerning location data relating to privacy, technology and policy-setting. The main contribution of this thesis is the development of a substantive theory grounded in empirical data from interviews, mobile phone location tracking and a survey. This theory is specific to a particular area, as it maps the relationship between mobile phone location data and perceptions of privacy within the UK.

The theory confirms some arguments in the literature that argue that the concept of privacy is changing with individuals' increased dependence on electronic communications technologies in day-to-day life. However, whilst individuals tend to hold a rather traditional picture of privacy, not influenced by technology and solely related to their own personal lives, scholars paint a picture of privacy that is affected by technology and relates to society as a whole. Digital mass data collections, such as communications data retention, are not perceived as privacy invasive by individuals. Mobile phone location data is not seen as related to a citizen's daily life but instead primarily as a crime investigation tool. A recognition and understanding of the divergence between the perceptions and definitions of privacy between individuals and the academic literature in relation to mobile phone location data is of relevance, as it should impact on future policies regulating the gathering, storage and analysis of personal data.

I confirm that the thesis is my own work; and that all published or other sources of material consulted have been acknowledged in notes to the text or the bibliography.
I confirm that the thesis has not been submitted for a comparable academic award.

…….

List of contents

List of Figures, Tables and Memos

Figures

Tables

Memos

Acknowledgements

I would like to thank a number of people that helped and supported me throughout my research, the data collection and writing up stages, without whom I would not have succeeded in completing such a rich study. I would especially like to thank the following:

First of all I would like to thank my supervisors Professor Antony Bryant and Dr. Edward Halpin, who have encouraged me to embark on this research project and have provided me with great support throughout my time as a PhD student. Particularly, I would like to thank Tony for encouraging me to use the grounded theory methodology and Eddie to direct my focus towards privacy. Further, I would like to thank Leeds Metropolitan University's Innovation North Faculty for providing me with the opportunity, resources and range of useful research seminars I enjoyed attending.

Special thanks goes to my respondents who gave their valuable time to be interviewed, to fill in my survey and to have the location of their mobile phones tracked. Great thanks also goes to all my friends and colleagues who spent many hours reading drafts of my thesis and giving me their valuable comments.

Finally, I would to say 'thank-you' to all my friends and family, particularly to my mother and late father, who have provided great support throughout the various stages of my work.

Glossary of Terms

1G: First generation mobile network or service; an analogue system.

2G: Second-generation mobile network or service. Generic name for second generation networks, for example GSM.

2.5G: *Second-generation enhanced*. Name given to enhanced 2G networks, for example GPRS and cdmaOne.

3G: *Third-generation mobile network or service*. Generic name for third-generation networks or
services under the IMT-2000 banner, for example W-CDMA.

3GSM: 3G services delivered over the evolved GSM core network (GSM Association proposes the universal adoption of this term).

Bit (binary digit): A bit is the primary unit of electronic, digital data. Written in base-2, binary language as a “1” or a “0”.

Bit/s: *Bits per second*. Measurement of the transmission speed of units of data (bits) over a network.

Bluetooth: A radio technology that makes possible transmitting signals over short distances between mobile phones, computers and other devices.

Bandwidth: The range of frequencies available to be occupied by signals. In analogue systems it is measured in terms of Hertz (Hz) and in digital unit and the size of which is independent of
redundancy or framing techniques.

Byte: (1) A set of bits that represent a single character. A byte is composed of 8 bits. (2) A bit string that is operated upon as a companies or between countries are not always meaningful.

CLI: Calling Line Identifier is the telephone number that a person has used to access their required service.

Coverage: Refers to the range of a mobile cellular network, measured in terms of geographic coverage (the percentage of the territorial area covered by mobile cellular) or population coverage (the percentage of the population within range of a mobile cellular network).

CCTV: Closed circuit television

Digital: Representation of voice or other information using digits 0 and 1. The digits are transmitted as a series of pulses. Digital networks allow for higher capacity, greater functionality and improved quality. Examples of digital cellular networks include GSM, CDMA, and TDMA.

Frequency: The rate at which an electrical current alternates, usually measured in Hertz (see Hz). It is also used to refer to a location on the radio frequency spectrum, such as 800, 900 or 1'800 Mhz.

GPRS: *General Packet Radio Service*. A 2.5G mobile standard typically adopted by GSM operators as a migration step towards 3G (W-CDMA). Based on packet-switched technology enabling high-speed data transmission (approx. 115 kbit/s).

GPS: *global positioning system,* refers to a "constellation" of 24 "Navstar" satellites launched initially by the United States Department of Defense, that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy ranges from 10 to 100 metres for most equipment. A European system, Galileo, is also under development.

GSM: *Global System for Mobile communications*. European-developed digital mobile cellular standard. The most widespread 2G digital mobile cellular standard, available in over 170 countries worldwide.

Hand-off (US) or Handover (UK): A central concept of cellular technology, enabling mobility for subscribers. It is a process by which the Mobile Telephone Switching Office passes a mobile phone conversation from one radio frequency in one cell to another radio frequency in another as a subscriber crosses the boundary of a cell.

HTTP: Hypertext transport protocol. A standard transport protocol for transferring 'web pages' from one machine to another.

Hz: *Hertz*. The frequency measurement unit equal to one cycle per second.

IMEI: *International Mobile Equipment Identity*. Unique serial number used on mobile phones, typically those connected to the GSM network.

IMSI: International Mobile Subscriber Identity, a unique number that is associated with all GSM and Universal Mobile Telecommunications System network mobile phone users. The number is stored in the Subscriber Identity Module (SIM).

IP: *Internet Protocol* Address. A numeric value that serves to uniquely identify an interface that is connected to the Internet.

ISDN: *Integrated Services Digital Network*. A digital switched network, supporting transmission
of voice, data and images over conventional telephone lines.

Location-based services (LBS): LBS make use of information on the location of a mobile device and user, and can exploit a number of technologies for the geographic location of a user. Some of these technologies are embedded in the networks and others in the handsets themselves. Location capability is already available to some level of accuracy (approx. 150 m) for most users of cellular networks. Increased accuracy can become available through location technologies such as GPS (Global Positioning System—see above). Commercial applications include the possibility for targeted advertising depending on the geographic region of a particular user.

Mb: *Mega bit*.

ITU: *International Telecommunication Union*. The United Nations specialised agency for telecommunications. See http://www.itu.int/.

m-commerce: *Mobile Commerce*. Similar to ecommerce but the term is usually applied to the emerging transaction activity in mobile networks.

Multimedia Message Service (MMS): MMS will provide more sophisticated mobile messaging than SMS. A global standard for messaging, MMS will enable users to send and receive messages with formatted text, graphics, audio and video clips. Unlike SMS, it is not limited to 160-characters per message.

PDA: *Personal Digital Assistant*. A generic term for handheld devices that combine computing and communication functions.

SIM: *Subscriber identity module* (card). A small printed circuit board inserted into a GSM-based mobile phone. It includes subscriber details, security information and a memory for a personal directory of numbers. This information can be retained by subscribers when changing handsets.

SMS: *Short Message Service*. A service available on digital networks, typically enabling messages with up to 160 characters to be sent or received via the message centre of a network operator to a subscriber’s mobile phone.

UMTS: *Universal Mobile Telecommunications System*. The European term for third-generation mobile cellular systems or IMT-2000 based on the W-CDMA standard.

URL: Unique/Uniform Resource Locator. A naming system for web resources.

USIM: *Universal Subscriber Identity Module* (card). A printed circuit board (similar to a SIM) that is inserted into a mobile phone. Adopted by W-CDMA operators for 3G mobile. Capable of storing much more information and has strong security functions compared with SIMs. Also referred to as *User Identity Module*, or UIM.

WAP: *Wireless Application Protocol.* A license-free protocol for wireless communication that enables the creation of mobile telephone services and the reading of internet pages from a mobile phone, thus being a mobile equivalent of HTTP (Hypertext Transfer Protocol).

Wi-Fi (Wireless Fidelity): Wireless systems that provide internet connectivity. Refers to Wireless Fidelity, the 802.11b specification for Wireless LANs from the Institute of Electrical and Electronics Engineers (IEEE). It is part of a series of wireless specifications which also includes 802.11a, and 802.11g.

Sources: International Telecommunication Union (2003)
and Home Office (2003b)

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 1 Introduction

1.1 Background to the study

The early part of the 21st century might be characterised as a period in which terrorism and the fear of terrorism have entered into the awareness and lives of a large number of people in the Western world. This in turn has made citizens increasingly aware of their own security and the British government of its need to provide effective measures to protect its people. The consequence of such protection might be an intrusion into areas of personal life that might once have seemed unacceptable. However, any attempt to strike a balance between competing interests is difficult, particularly in a technologically fast-changing environment. It is in this complex context that this research is based.

The mobile phone has become an omnipresent communication technology within our society and can be found in the pocket of almost everyone, from children to their grandparents, from senior managers to cleaners. It has an immense impact on our social lives and how we interact with other people. There are over 65 million mobile phone subscriptions in the UK (Mobile Operators Association, 2006) for an estimated UK population of 60.2 million (National Statistics, 2006). The ubiquitous mobile phone can also be seen as being Janus-faced - as having two sides with opposing attributes. On the one hand, mobile phones connect people and enable social interactions in a way that has not been possible before. On the other hand, the mobile phone has the capability to act as a universal tracking device on an individual basis. Every mobile phone routinely generates a host of data including its approximate geographical location. This data is known as *mobile phone location data* and is typically based on the nearest mast from which the handset receives a network signal. Location data, together with other data about communications, is stored by mobile phone service providers for billing and legal purposes. This communications data includes details such as the location from which phone calls are made, duration and destination of calls. It is used regularly in court cases and by the intelligence services as it provides a rich picture about a mobile phone user's actions (Walker and Akdeniz, 2003; Green and Smith, 2004). Without technological

developments such as faster computer processors, increased storage capacities and networked technologies, today's large scale collections of personal data would not be possible. The changing nature of computing technologies has resulted in the increased digitisation and routine generation of data, as well as its long-term storage and analysis. Converging platforms and infrastructures, such as the internet and mobile phones, increase the sensitivity of the data generated, as for example when mobile phone handsets are used to access the internet (Escudero-Pascual and Hosein, 2004).

The Surveillance Studies Network (2006) raises concerns that the routine tracking and information gathering mechanisms used in today's society are often not obvious to citizens. This makes it important to incorporate checks and safeguards when collecting data to ensure accountability. Especially the retention of mobile phone communications data bears the potential for identifying patterns in the collected data. It is possible to analyse the behaviour of particular groups of people or of mobile phone users located in a particular area, without identifying specific individuals
(Marx, 2002). Britain's Information Commissioner, has used the term 'surveillance society' to express his concerns about the vast majority of citizens being subjected to frequent collections of personal data on a day-to-day basis (Surveillance Studies Network, 2006). "Everyday life is subject to monitoring, checking and scrutinising", states Lyon (2001, p. 1). Dandeker (1990) argues that information systems equal surveillance systems, as surveillance can be interpreted in the broad sense of gathering information about individuals and populations. Hence, the term *surveillance society* should not merely be perceived in the context of totalitarian regimes or regarding a centralised Orwellian 'Big Brother' figure but rather as relating to the continuous gathering of information facilitated by networked computer systems.

Webster (1995) emphasises the role of routine surveillance as a prerequisite of effective social organisation. He offers the example of supermarket shopping as an enormous organisational achievement, which would not be possible without the support of technologies to coordinate the daily routine of producers, suppliers, transport and customers. However to organise life, information must be systematically gathered on people and their activities, it needs to be known what is required and this can be interpreted as surveillance. Indeed, surveillance systems are necessary to ensure that citizens are paid correctly, receive state benefits, can

vote in elections and assist with crime and terrorism investigations (Lyon, 1994). Bureaucracy is a means to manage affairs in more efficient ways and involves systematic book keeping, building up of records, rules and procedures, as well as documentation of cases (Webster, 1995). "The age of bureaucracy is also the era of the information society" as Dandeker (1990, p. 2) convincingly observes. He perceives bureaucracy as a highly effective method of exercising surveillance over subject populations in industrial societies. The increased use of IT-based surveillance can be seen as a response to risk, with the aim to achieve the pro-active management of threats. Several underlying trends of Western societies have facilitated the notion of the surveillance society, such as the need to manage risks in order to deal with internal but also external threats in form of terrorism, as well as the growing routine generation and subsequent use of citizens' personal data (Surveillance Studies Network, 2006).

Beck (1992) describes the consequences of industrial and scientific development as consisting of risks and dangers that society has not previously faced. Dangers are not only defined as naturals hazards such as storms and earthquakes but instead the use of modern technologies and science has created additional, man-made hazards. Consequently, Beck characterises the risk society as driven by the distribution of 'bads' or dangers, as opposed to the industrial society, which was primarily concerned with the production of 'goods'. Even though Beck mainly had environmental 'bads' or negative effects of the modern society in mind, this also applies to social and political 'negatives', as resulting from routine tracking of communications data. Ericson and Haggerty (1997) share Beck's view and argue that "risk is a central feature of modernity". The risk society is a society that is organised in response to risks and governments are concerned with providing security. It is underpinned by a collective fear and a continual need for more knowledge of risk in order to obtain greater powers to reduce risk. Routine surveillance of everyday actions and communications enabled by networked technologies facilitates the categorising of individuals and populations with the aim to classify them in terms of potential risk. The accumulation and subsequent analysis of communications data, including mobile phone location data, can be seen as an aspect of the pro-active management of risks.

Despite the positive aspects of technologies to facilitate the coordination and organisation of day-to-day life, as well as the use of IT-based surveillance to respond to social disorder and rising crime levels, Davies (1996) warns of the

surveillance mechanisms made possible by computers. He believes that linking computer systems to share information about citizens facilitates the potential of misuse by governments and the private sector. The constant surveillance of citizens may result in mistrust and could distance the citizen from the State. Some fear that communications data may be used by law enforcement for social sorting, in other words the differential treatment for different categories of persons as already performed with existing data (Lyon, 2005). Knowing a person's location at any given moment in time can have implications for privacy, civil liberties and social justice. The retained location data can be used to analyse past movements and communication routines of a person, as well as predict potential future behaviour, which can have negative consequences for the individual (Clarke, 2000; Lyon, 2005). Hence, the purposeful, routine and systematic generation of individuals' personal details can have an impact on the privacy of those whose information is being gathered. Clarke (1999) claims that privacy is important from a political viewpoint, enabling freedom of speech to think and act. In his view, the monitoring of individuals' communications and actions threatens democracy. Taylor (2002) argues in a similar fashion that considerable advances in technology have increased the powers of governments to carry out surveillance upon its citizens. While Lyon (1994) believes that it is not the widespread adoption of information and communication technologies which has resulted in a "totally new situation" but that technologies merely facilitate and accelerate the trend towards a surveillance society.

Location technologies pose new challenges for privacy policy and law. Parallels with already existing surveillance in the form of recording of internet data, CCTV footage or consumer data, suggest that location data is valuable to various stakeholders and has the potential for commercial applications. Bennett and Crowe (2005, p. 1) argue that location is the "new dimension to the privacy problem", as now surveillance is not only about who citizens are and what they are doing but also *where* citizens are taking actions that may be of interest to law enforcement and commercial actors. The monitoring of location data enables mobile surveillance, which is of significance as individuals are on the move in their professional and personal lives, representing the mobility of modern society. Location becomes a significant source of valuable information in itself (Bennett and Regan, 2004). The attribute location can offer many opportunities to businesses, governments and individuals. However, a distinction needs to be made between the use of data for law enforcement and for commercial purposes when looking at the relationship between mobile phone

location data and privacy. The role of individuals as consumer and as citizens differs from a legal point of view. The use of communications data by the government falls under state surveillance techniques and is regulated by legislation such as the Regulation of Investigatory Powers Act 2000 (see section 2.3.3.2), whereas the use of communications data for commercial services is for example regulated by the European Union Electronic Communications Privacy Directive (Directive 2002/58/EC).
Governments have recently amended their legislative approaches to retention and access of communications data. This had been in response to threats resulting from criminal acts using technology and also the need to take into consideration the case law of the European Court of Human Rights. A right to privacy is enshrined in the European Convention on Human Rights (Article 8) and is brought into British legislation in form of the Human Rights Act 1998. Nevertheless, this 'right to private life' (Article 8.1) may be compromised if seen as necessary under a range of exclusive purposes listed in Article 8.2 ECHR, such as national security (see section 2.2.1). In addition, the September 11 attacks in the US in 2001 have brought about a paradigm shift in Europe regarding the legislation of storage and access of communications data (section 2.3.3). In the United Kingdom data retention laws require mobile phone service providers to store communications data for 12 months on a voluntary basis (Home Office, 2003c, section 16). A European data retention Directive requires the implementation of a data retention regime by all member states by 2007, which however may be postponed in relation to “the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail” by individual member states until 2009 (Directive 2006/24/EC, 2006, Article 15).

Attention needs to be drawn in this context to the distinction between the concepts of privacy and security. *Privacy* can relate to the control over personal information, for example the commercial misuse of customer data. Privacy has been declared a fundamental human right by the United Nations Universal Declaration of Human Rights (see section 2.2.1), whereas *security* is concerned with the safety of information exchanged, possible loss and unauthorised access. Security constitutes a critical part in privacy protection but does not play a major role in this research investigation.

1.2 Research rationale

The mobile phone is a ubiquitous tool in today's society, a daily companion for the majority of British citizens. However, the ability of mobile phone networks to trace a mobile phone's geographic position at all times generates potentially sensitive data that can be stored or shared for significant lengths of time. The continuous generation of mobile phone location data, besides other communications data shows that the mobile phone can also be a very privacy invasive technology, as it blurs the boundaries between different areas in life, such as family and work life. Communications data from mobile phone conversations is retained for ordinary citizens as well as for criminals on a long-term basis, including the geographical location from which the phone call was made. Mobile phone location data encompasses private and public spaces, it allows intrusions into traditional private areas like homes.

An individual's use of mobile phone services falls under the protection of the 'respect for privacy life', as enshrined in the ECHR under Article 8. This extends to the right of citizens to establish and develop relationships with other human beings (Whitty, Murphy and Livingstone, 2001). Therefore the long-term retention of all mobile users' communications data may be seen as violating some of the most important rights that a democratic society must defend: the right to privacy, freedom of expression and the presumption of innocence (section 2.2.3.1).

Looking at the wider picture, location data can be seen as just one type of data that is collected about a person beside other data such as CCTV footage or financial data. However, location data differs as it tends to be specific to one person and is collected continuously, particularly if the mobile phone is carried by its user all day, every day.
The focus of this research is on *location* data*,* as opposed to communications data in general (for more detail see Chapter 2, Part 3 Legal framework). The reason for this is that the relationship between location and privacy has so far received very little attention in the academic literature. Location is "a new dimension to the privacy problem" according to Bennett and Crowe (2005). It is certainly to become more important in the future, taking into account the increase of networked and location-aware technologies, such as Bluetooth, RFID and Wi-Fi (for details about these terms see Glossary, p. xiii).

Existing comparable studies have either examined mobile phone users' behaviour or attitudes towards privacy in general. Over the last decades numerous studies have looked at citizens' and consumers' attitudes towards privacy (see Zureik, 2004). The motivations for these studies have either been of a commercial or a political nature. The studies mainly use questionnaires and quantitative data in order to focus on public attitudes on a large scale and hence cannot explore individuals' perceptions in-depth. Much popular literature refers to location-based services as the 'new big brother' (see for example Spinney, 2004). Data identifying an individual's location with the help of electronic devices has been considered in the literature regarding a range of technologies other than the mobile phone, for example GPS (Monmonier, 2002; Van Riper and Whitfield, 2004), Wifi (Hosein and Escudero-Pascual, 2002; Varshney, 2003) or digitised financial transactions (Clarke, 2000).

Academic literature has predominantly considered mobile phone location data in relation to the technical aspects in mobile phone and internet systems, including security (Drane et al., 1998; D'Roza, 2003; Beresfod, 2005; Steiniger et al., 2006; SnapTrack, 2003), or reviews legal implications of communications data in general (White, 2003; Escudero-Pascual and Hosein, 2004) or specifically regarding the UK (Green and Smith, 2004; Whitley and Hosein, 2005). Some literature focuses on particular areas of location monitoring such as for emergency services (Gow, 2004), employee monitoring (Kaupins and Minch, 2005) and children tracking (Mathieson, 2004), and mostly in the country-specific contexts of Canada (Lyon et al., 2005; Bennett and Crowe, 2005) and the US (CDT, 2006).

The particular strength of this study is its focus on empirical evidence which brings together individuals' attitudes towards location data and their perceptions on the data's implications on privacy. This study has followed Woolgar's call for the assessment of underlying assumptions in social research related to modern technologies. Woolgar (2002, p. 7) encourages researchers to "disaggregate the phenomenon, to focus more on bottom-up experiences" and to find out how technologies are used and experienced in everyday life. This appeal for empirical data collection is echoed by Bennett (2005) and Marx (2006) who suggest conducting more empirical investigations, and argue that assumptions about technologies and their potential for surveillance practices need to be critically examined. Lyon (2001, p. 146) warns that "political questions fail to connect with the world we live in", because too little attention is paid to "actual empirical realities".

1.3 Aims and objectives

The overall aim of the research project has been to investigate the implications of mobile phone location data on individuals' perceptions of privacy. It has *not* been the aim to develop a conceptual framework for analysing the privacy and surveillance implications of mobile phone location data or to draw final conclusions about the condition of individuals' perceptions of privacy. Instead, the voices of ordinary citizens have been heard, when expressing their views regarding mobile phone location data and communications data retention. Grounded theory methodology (GTM) was used to illustrate patterns and themes that are useful in understanding the broader discourses concerning location data relating to privacy, technology and policy-setting.

The five main objectives to advance the research aim are presented below,

Objective 1 - to investigate individuals' awareness of and attitudes towards mobile phone location data.
It is important to portray and to represent the needs of ordinary citizens in the complex debate about technological influences on individual privacy, since the views of citizens can and should have an effect on future policies regulating the gathering, storage and analysis of personal data (Surveillance Studies Network, 2006). In order to learn about citizens' awareness of location data and its impact on people's everyday lives, a number of empirical data collections, in form a location-tracking pilot study, a survey and a series of interviews will be conducted. The methodology to guide the collection of data will be discussed in Chapter 3, and the findings from the data collections are presented in Chapter 4.

Objective 2 - to provide a suitable background to the subject area of mobile phone location data and communications data retention in general.
In order to fulfil the second objective, it is necessary to identify and discuss the current technological background regarding mobile phone location data within the UK. This will be supplemented by a review of relevant legislative developments, as well as the representation of privacy in the literature. The objective will be met by conducting an extensive review of the relevant literature, which will be provided in Chapter 2.

Objective 3 - to identify the positions of the different stakeholders involved, such as the UK and EU governments, mobile phone service providers, and individuals.

This objective seeks to paint a picture of the dynamics in developing the regulative framework for communications data retention, while considering the view points of the various actors. The objective is predominantly addressed in Chapter 2 by a literature review, and in Chapter 5, where empirical findings are related to the relevant literature. A limited number of interviews with experts in the area supplement the review of the literature.

Objective 4 - to analyse the relationship between individuals' perceptions, and the relevant literature regarding mobile phone location data.

As part of this objective, privacy definitions commonly used in and known from the literature will be critically evaluated in the light of the analysis of empirical data. Discrepancies between the respondents' views of privacy and those represented in the relevant literature will be identified and discussed. This takes place in Chapter 5, where also the relationships between the grounded theory categories are explicated.

Objective 5 - to offer an explanation about the phenomenon under study: individuals' views of privacy in relation to mobile phone location data.

The final objective will be achieved by developing a theoretical model in the form of a grounded theory, which will map the relationship between mobile phone location data and individuals' perceptions of privacy. The theory will be based on the grounded theory categories and the relationships between them. The objective will be addressed in Chapter 5.

1.4 Methodology overview

Central to this research was the choice of methodology. Grounded theory methodology is a methodological tool that offers a framework for qualitative analysis and can be used to develop new theory based on the collected data. For this study, initial data was gathered with the help of a pilot study, which involved identifying the geographical location of participants' mobile phones and eight semi-structured interviews. Ten further in-depth interviews and a survey have been conducted to examine individuals' perceptions of privacy regarding mobile phone location data (see Table 1.1). All interviews were coded and analysed using grounded theory methodology. The study does not make use of predefined theoretical frameworks as a starting point but instead used an inductive approach to explore this research area from a fresh angle. The lack of existing theory regarding mobile phone location data and privacy justified the use of GTM as a suitable research methodology.

Table 1.1: Steps in data collection

Data collection
Interview phase 1 + Mobile phone location tracking pilot study - Conduct and transcribe 2 x 4 Pilot study interviews - Track location of 5 mobile phones over 4 weeks
Interview phase 2 - Conduct and transcribe 5 in-depth interviews
Survey - Develop and test pilot questionnaire - Distribute questionnaires paper-based and online, 477 respondents
Interview phase 3 - Conduct and transcribe 5 in-depth interviews
Analysis - Develop final categories, based on codes and grounded theory memos - Triangulate findings from pilot study, interviews and survey and compare to literature.

1.5 List of publications

Paper title: 'Monitoring individuals' movements - is mobile phone location data a threat to individuals' privacy?', presented at the Young Researchers' Seminar 'The Passenger as a Risk: Monitoring Movement and Privatising Threat', Law Faculty of the Radboud University Nijmegen, NL, 15 and 16 March 2007

Presentation 'Implications of mobile phone location data on individuals' perceptions of privacy in the UK - a Grounded Theory study', discussed at the SECURINT Summer School, Strasbourg, France, 17th to 21st July 2006

Presentation with the title 'Implications of mobile phone location data on individuals' perceptions of privacy - a Grounded Theory study' at the Faculty of Innovation North Conference, Leeds Metropolitan University, Leeds, UK, July 2006. [Internet] *http://www.leedsmet.ac.uk/inn/research2006.htm*

Presentation with the title 'Mobile phone location data and individuals' perceptions of privacy - a Grounded Theory study' at the Postgraduate Conference, Leeds Metropolitan University, Leeds, UK, May 2006. [Internet] *http://www.leedsmet.ac.uk/research/postgradconf/papers.htm*

Presentation and paper with the title 'Mobile Phone Location Data - Personal Privacy vs. National Security' Netties Conference, Austria, October 2005. [Internet] http://www.netties2005.at

Presentation with the title 'Mobile Phone Location Data - Personal Privacy vs. National Security' Faculty of Innovation North Conference, Leeds Metropolitan University, Leeds, UK, July 2005. [Internet] *http://www.leedsmet.ac.uk/ies/INNResearchConf05.htm*

Poster 'Impact of Mobile Phone Location Data on Individual Privacy' presented at The 5th Social Study of IT workshop at the LSE, Mobile Interaction: Individuals, Organizations and Infrastructures. Poster Session, London School of Economics, London, UK 4-5 April 2005.

Poster 'Impact of Mobile Phone Location Data on Individual Privacy' presented at the Poster competition UK Grad, Leeds University, Leeds, UK, May 2005

Paper 'Tracking me, tracking you – an observational study exploring mobile phone location data and privacy' published in Research in progress papers 2004, Leeds Metropolitan University [Internet].
http://www.leedsmet.ac.uk/inn/documents/RIP2004-10.pdf

Presentation ‘Tracking me, tracking you – an observational study exploring mobile phone location data and privacy’ at the Technologies: Studies and Strategies, Postgraduate Research Conference. 9th December 2004, University of Surrey, Guildford, Surrey, UK. [Internet]
http://incite.surrey.ac.uk/pgconference/conference_programme.htm

Presentation ‘Your Mobile Phone - a companion betraying your privacy?’ at the ICT+ Faculty Research Conference, Leeds Metropolitan University, Leeds, UK, July 2004. [Internet] *http://www.lmu.ac.uk/inn/ICT_conference.htm*

1.6 Guide to subsequent chapters

The thesis consists of six parts: 1. Introduction, 2. Literature Review, 3. Methodology, 4. Presentation of data, 5. Discussion and analysis of findings, and 6. Conclusions and Recommendations.

The purpose of this introductory chapter, **Chapter 1**, is to set the scene for the thesis by describing its overall context and rationale, including aims and objectives. **Chapter 2** reviews the relevant literature, which is grouped into three strands significant to the research area: first, mobile phone technology with a focus on location data, second, definitions of privacy in the literature and third, the legal framework relevant to mobile phone location data. The methodological paradigm adopted for this study is described in detail in **Chapter 3** along with the rationale for this choice. Grounded theory methodology has directed the methods used for data collection and is central to the way in which this thesis examines the empirical evidence. Interview questions for each of the three interview phases, screenshots of mobile phone location tracks and a copy of the questionnaire are provided in the Appendices A to L and referred to in the chapter.
Chapter 4 reports the outcomes of the empirical data collection. The findings are presented with reference to the different stages of data collection: pilot study, in-depth interviews and survey. Codes, memos and visual displays of ideas provide an insight into how each of the five final categories was developed.
Chapter 5 is divided into three parts. Part 1 draws together and triangulates the results from the different data collection methods. Empirical findings are contrasted with the literature and synthesised in order to provide a holistic interpretation of the research question. A theoretical model is presented depicting the implications of location data on individuals' perceptions of privacy. Part 2 of Chapter 5 presents the four main findings developed from the categories and illustrates the relationships between the categories. Part 3 explains the divergences between individuals' views of privacy and those predominantly discussed in the literature.
The final chapter, **Chapter 6**, sets out the conclusions drawn from the study in relation to the aims identified above. It draws all data and interpretation together and makes suggestions for further research.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 2 Literature review: Privacy, Mobile phone technology and Legal framework

When examining the subject area of communications data retention broadly three areas need to be taken into account: a) technological matters, b) social values such as privacy and civil liberties, and c) law enforcement issues (Whitley and Hosein, 2005; Raab and Bennett, 2006). Accordingly this chapter has been divided into three parts; the first part focuses on the role of geographical location within mobile phone technology, the second part discusses the relevant privacy related literature, and the final part of this chapter examines the legal framework relevant to mobile phone location data.

Grounded theory methodology has been used to guide collection and analysis of empirical data for this study (for more detail see Chapter 3 - Research Methodology). GT methodology is an inductive method, which means that typically only a very broad review of literature takes place before collecting the data. However in addition to this initial review, the literature is visited again *after* the data collection has been completed. This study has followed this approach with the benefit that a second review of the literature could be guided by findings from all three empirical data collections - pilot study, interviews and survey. Particularly the development of the final GT categories, which was supported by written and visual memos, has prompted the review of further literature.

The literature discussed in this chapter is a result of this iterative process and some literature particularly relevant to the findings from study will be revisited in Chapter 5 and brought into relation to the empirical findings.

2.1 Part 1: Mobile phone location data

This section presents essential technical background to mobile cellular networks in order to provide an understanding of the role of location data. A brief history of mobile phone telephony is provided and followed by an explanation of the relevance of the cellular network architecture to mobile phone location data. Following this a technical overview of mobile communications network architecture is provided and finally location-based services and techniques of locating a mobile phone are discussed.

2.1.1 Background to mobile phone location data

The mobile phone is a key technology in an increasingly mobile and connected world. Growing technological convergence and ubiquitous networking leave behind a continuous and lasting trail revealing information about those involved in the communication. Picking up on this electronic trail makes it possible to identify the location of communication devices and individuals are indirectly locatable by carrying their mobile phone. In some cases, the location information supplied by a mobile phone can be very specific, depending in cell size and cell shape, which will be explained later in this section. Location-based services (LBS) for mobile phones (see section 2.1.3) are predicted to grow in the near future (see Lyon, 2005). A market research firm predicts that LBS revenues will reach €622m by 2010 (Moore, 2006).

The mobile phone as a location technology brings together the following three key features:

1) identification of the approximate location of the handset
2) on a continuous basis
3) in real-time

The combination of these features means that mobile phone users can potentially have their geographical location and movements traced at any time or all the time. In addition, a log of all data generated by a mobile phone is stored by the mobile phone service provider, and potentially shared, as discussed in the final part of this chapter (2.3 Part 3: Legal framework relevant to mobile phone location data). This makes the mobile phone unique in comparison to other location identifying technologies, such as CCTV or RIFD, particularly as a mobile phone tends to be carried by one person on a regular or sometimes even continuous basis. CCTV for

example can track individuals in real time but not continuously, RFID tags can also reveal location information but tend not to do this in real-time or o a constant basis. WiFi networks can also be used to locate the position of the device connecting to the wireless network (Hosein and Escudero-Pascual, 2002). However, this is limited to the size and the geographical area covered by this network.

Location data can be perceived as both a threat and an opportunity. There are many opportunities that the attribute location can offer to businesses, governments and individuals. However, knowing a person's location at any given moment in time can also have implications for privacy, civil liberties and social justice (Clarke, 2000; Lyon, 2005).

2.1.1.1 History of mobile phone telephony

The development of wireless communication systems started in the 1930s with the use of 'Walkie-talkies' during the Second World War to enable foot soldiers to stay in contact with the headquarters (Elliott and Philips, 2004). In 1946, AT&T Bell introduced the first commercial radiotelephone service in the US, which allowed communication between mobile users in cars and the public fixed network.. In the 1960s, Bell Systems launched the Improved Mobile Telephone Service (IMTS), which laid the basis for commercial-sector mobile communications. Developments in microprocessor technologies in the late 1970s and early 1980s enabled the introduction of the reliable wireless communications system, the so-called first generation.

First generation network - 1G

The first generation wireless technologies, also known as 1G, were relatively simple and used analogue signals. Mobile phone handsets based on 1G technology were mainly used by government agencies and the military before this technology came into general use in the business domain in the 1980s (Elliott and Philips, 2004). The systems in Europe and the USA had in common that they provided coverage of a very large area by using only one transmitter mast. The coverage area of a mast was fairly large, up to 150km, and required minimal infrastructure. In order to connect via large distances, the base station as well as the mobile phone had to transmit simultaneously at high power. This meant that the mobile phones were larger than today's handsets and used to be built into car boots. Moreover, due to the limited number of available frequency channels, only a small number of

subscribers could be connected to the mobile phone network (Walke et al., 2003). 1G systems were based on analogue signals which are radio transmissions sent in a wave-like form. The mobile device sends the waves to a base station where the signal is reconstructed as accurately as possible and relayed to its destination. Noticeable differences in quality occur due to errors recreating the signal wave. In addition, analogue signals are relatively easy to intercept, as they are transmitted in the clear (Deitel et al., 2002).

Second generation networks - 2G

In the late 1980s and early 1990s, the popularity of wireless communications grew and increased the demand for network capacity. Together with the disadvantages of analogue 1G systems, this led to the development of the second generation wireless system based on digital technology. Digital signals have different transmission properties than analogue signals and use binary coding using sequences of 0s and 1s to construct a signal's unique pattern. Digital signals use digital samplers and codecs to convert analogue voice data into digital data. Digital signals can be precisely duplicated by the receiving base station and send to its destination. This process results in a lower error rate than analogue transmission correction which results in clearer voice reception (Deitel et al., 2002). In addition, digital traffic is relatively simple to encrypt in order to prevent eavesdropping (Stallings, 2005).

GSM, the Global System for Mobile Communications, fundamentally differs from the 1G system because of its use of cellular network architecture, which will be explained in subsequent sections. GSM, also known as second generation network or 2G, was first developed in the 1980s through a pan-European initiative, involving the European Commission, telecommunications operators and equipment manufacturers. GSM is an open non-proprietary and interoperable digital standard for cellular mobile systems operating in the 900 and 1800 MHz band. In 1986, a number of different prototype systems put forward by companies and consortia from different European countries were trialled and led to the agreement of the main characteristics of the new system (Steele et al., 2001).

GSM is still in use to date by all European countries and has also been adopted in other continents, such as Africa and South America. There are over 540 million GSM subscribers in Europe, plus another 18 million Europeans using 3GSM networks, which are the 3G service delivered over the evolved GSM core network

(GSM Europe, 2005). With GSM it was also made possible to send and receive limited amounts of data via the Short Messaging Service (SMS) and mobile internet browsing via the wireless Applications Protocol (WAP) (Elliot and Philips, 2004).

Second and a half generation networks - 2.5G

2.5G technologies represent a state of development between 2G and 3G and have overcome the limited data and primarily voice-centred services of the 2G networks. In the 1990s and early 2000s higher transmissions rates and always-on connectivity were enabled by General Packet Radio Services (GPRS). Data transmission speeds were now 10 times faster with 115kbits per second and based on packet-switching technology (International Telecommunication Union, 2003). Packet switching optimises the use of bandwidth available in a network and minimises the time it takes for data to travel across the network. The increased data transmission rates of 2.5G compared to earlier systems help to transfer data such as mobile internet content (Elliot and Philips, 2004)

Third generation networks - 3G

Third generation mobile telephony (3G) is the successor to the 2G and 2.5G systems. 3G improved previous systems by providing enhanced security and encryption features, improvements in screen displays and the ability to handle multimedia data, such as graphics and video streaming. 3G allows faster data exchange with data transmission rates up to 1920kbits per second, which enables the support of greater voice and data customers. Support can be provided for a wide variety of mobile equipment. 3G technologies were first introduced in Japan in 2001 and spread to Europe and the USA in 2002. UMTS (Universal Mobile Telecommunications System) is the third generation mobile phone technology mainly used in Europe and also in Japan. It uses the GSM infrastructure and UMTS/GSM dual-mode phones sold in Europe are able to make and receive calls on both networks. Elliott and Philips (2004) describe as aims of all 3G networks the following:

a) world-wide connectivity and roaming throughout Europe, Japan and North America
b) high data transmission rates and broad bandwidth, suitable for multimedia content
c) efficient spectrum utilisation

(Philips and Elliot, 2004)

2.1.1.2 The cellular concept

In terms of location data the most crucial concept was the introduction of the cellular network architecture with the change from the 1G to the 2G system. In 1972, a patent was registered by Bell Labs, the research subsidiary of the US telephone company AT&T that laid the foundations for today's second and third generation mobile phone systems (US Patent full-text and image database, 1972). The essence of this patent was to reduce the area covered by an antenna. In the 1G system, only one antenna served a very large area, whereas in the 2G this area was broken down into several cells.

Each area or cell is served by a single base station and is in the approximate centre of each cell. Due to the increased number of cells in the 2G system compared to 1G, many more masts were needed and this enormously increased the costs of infrastructure. Now it was possible to reuse the same frequency over relatively small distances, enabling coverage for a greater number of subscribers. This resulted on the one hand in the reduced size of antennas, and on the other hand in reduced distances between antennas. Another effect of this new system was that the long-distance transmissions between mast and handset were not necessary anymore, which resulted in decreasing sizes of mobile phone handsets and improved handset operating times. Adjacent cells cannot use the same frequency, as this could result in interference. Hence, it is necessary to only re-use frequencies in cells that are sufficiently distant to each other. The transmission power of a base station has to be limited to prevent interference with frequencies from other cells and to reduce health concerns (Stallings, 2005).

This concept of using an increased number of smaller cells required a mechanism to switch a user's connection from cell to cell. Hence, cells were arranged in a hexagonal pattern to enable all antennas to be the same distance apart, which is beneficial when a mobile phone user moves within a cell towards its boundary. This makes it easier to determine when to switch a user to an adjacent antenna and which antenna to chose. In comparison a square pattern, would only provide an equal distance to the centre of four cells (see Figure 2.1).

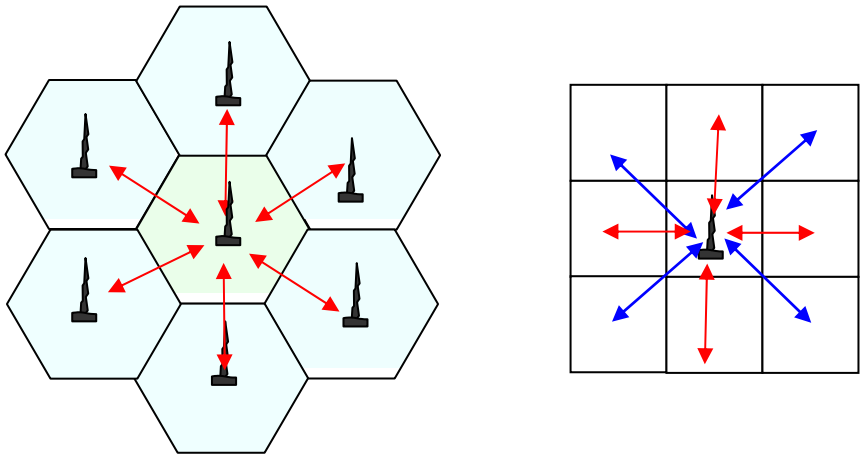


Figure 2.1: Contrasting hexagonal and square pattern (after Stallings, 2005)

In practice, cells have irregular shapes and a precise hexagonal pattern is often not used due to topographical limitations, restrictions on positioning antennas and different amounts of traffic volumes as some cells have more mobile phone users than others. In addition, the coverage can overlap in looser shaped cells (Philips and Elliot, 2004). Different shaped cells have an impact on the accuracy of mobile phone location tracking based on the Cell-ID, as smaller cells provide a more accurate result than larger cells.

2.1.1.3 Increasing the capacity of a mobile phone network

There was a considerable increase in the proportion of households with a mobile phone since 1998-99 from 27 percent to 78 percent in 2005 (National Statistics (2005). The increasing number of mobile users has caused the necessity to enhance the network capacity. According to the Mobile Operators Association (2006), base stations can only carry a maximum of around 120 calls at the same time.

A mobile phone network can be made suitable for an increased number of phone users in several ways:

- Add new channels (if possible)
- Frequency borrowing from adjacent cells
- Cell sectoring
    - divide cell into wedges, each with own channels (usually 3 or 6 sectors per cell)
    - each sector has its own subset of channels
    - the base station has to use directional antennas
- Cell splitting
    - generally cells are 6.5 to 13km in size
    - power level of antenna is reduced to keep signal within cell
    - since the cells are smaller, more frequent handovers (i.e. transfer of call from one Base transceiver to another) have to take place
- Micro cells
    - Antennas move lower down, e.g. from top of buildings to smaller buildings or lamp posts
    - Cell size is decreased and a reduction of power takes place
    - Micro cells are usually in place on the high street where great traffic volume can typically be found
    - 10 - 400 metres radius circle

(Stallings, 2005)

To summarise, due to an increasing number of mobile phone users, more mobile masts have been put up. This has resulted in smaller cells that can cope with the higher traffic volumes. In some cases, citizens have raised protests against new masts being put up in residential areas mainly due to concerns about health risks originating from the base stations (Mast Sanity, 2006). The use of smaller cells leads to a higher accuracy for mobile phone location identification based on Cell-ID.

Even though this is not the most accurate method, the cell-id or mast in use is a pre-requisite for more accurate ways of determining a handset's location (as discussed in section 2.1.4, below).

2.1.1.4 Health concerns in mobile telephony

Health concerns are based on the radiation emitted by mobile phone handsets and base stations. The latter emits radiation continuously and much more powerfully. An independent expert group on mobile phones (IEGMP), also known as the Stuart Group, was established by the Minister for Public Health Tessa Jowell in 1999 to consider concerns about possible health effects from the use of mobile phones and bases stations (Independent Expert Group on Mobile Phones, 2000). The report concluded that no clear indication of short and medium term health hazards could be found. A precautionary approach to the use of mobile phone technologies was recommended until more scientific evidence was available. A more recent report by the board of National Radiological Protection Board states that “the main conclusions reached in the Stewart report in 2000 still apply today” (National Radiological Protection Board, paragraph 19, 2004).

2.1.2 Technical overview of mobile communications support

An essential part of a mobile phone network's tasks is to monitor the location of every registered mobile phone device, as mobile phone users are free to roam throughout the coverage area of a cellular network. Therefore the network must possess some way to track mobile phones so that it can successfully route incoming calls and text messages to them. Mobile phone location data is an inherent feature of mobile communication and for this reason some technical background to mobile communication is provided in this section. At first the interplay between mobile phone handset and mobile phone base stations is explained, followed by what happens when a call takes place. It should be noted that this section only touches on the general principles of mobile communications based on cellular wireless networks. Detailed technological developments are not described here as they are not of relevance for this study.

2.1.2.1 Overview of the cellular network architecture

The GSM network architecture consists of three parts which are essential to enable mobile communication: the mobile phone handset, the base station and network subsystem. Each of these elements of a mobile phone network is described in more detail in subsequent sections to explain how the position of a mobile phone handset can be identified. See Figure 2.2 for an overview of the key elements of a cellular network. A mobile phone network continuously generates a host of information which is stored in various databases. The most relevant databases for determining a mobile phone handset's location are the visitor location register (VLR) and home location register (HLR) database.

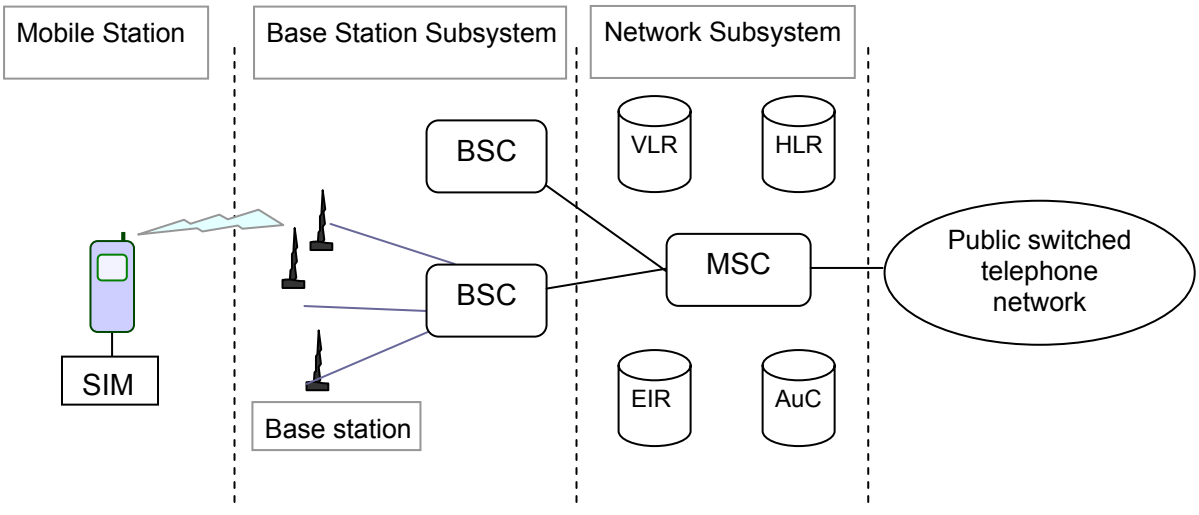


Figure 2.2: GSM network architecture (after Walters and Kritzinger, 2000; Walke, 1999)

Mobile phone handset and SIM card

A mobile phone handset contains a radio transceiver, digital signal processors and a removable smart card, known as subscriber identity module (SIM). The SIM card can be transferred between handsets and contains the international mobile subscriber identity (IMSI), which is used to identify the subscriber to the system. The mobile phone handset or device is uniquely identified by the IMEI number (International Mobile Equipment Identity) and depending on the mobile phone contract personal details about the user are known by the service provider. Customers of monthly paid contracts need to register their personal and bank details with their service provider, whereas for a pre-paid contract registration is not always necessary (Stallings, 2005).

Base station subsystem: Base station (BS) and base station controller (BSC)

The base station subsystem (BSS) is responsible for handling traffic and communications between a mobile phone and the network subsystem. The BSS consists of two elements, one or more base station transceivers (BST) (commonly referred to as mobile phone masts) and the base station controller (BSC).
Each base station transceiver includes a radio antenna which handles the radio-link protocols with the mobile phone and a link to one of the base station controllers and is assigned to a single cell. The base station controller manages allocation of radio channels, reservations of radio frequencies and handovers of mobile phone handsets from one cell to another within the BSS. The BSC can either be located with a BST or can control multiple BST units, hence serves multiple cells. A group of BSCs is connected to a mobile switching centre (MSC) via microwave links or telephone lines (Hubaux and Znaty, 2000; Steele et al., 2001).

Network subsystem: MSC, HLR, VLR, AuC, EIR

The network subsystem (NS) provides a link between the cellular network and fixed networks such as the analogue public switched telephone networks (PSTN) or digital integrated services digital network (ISDN). The NS controls handovers between cells in different base station subsystems, authenticates users and validates their accounts. It also provides functions for worldwide roaming of mobile users. The main part of the network subsystem (NS) is the mobile services switching centre (MSC), which is supported by the following four databases that it controls.

a) Home location register database (HLR)

The home location register database (HLR) contains an entry for every SIM card issued, including details such as telephone number, mobile equipment number, equipment type and subscription type. Typically, GSM networks have only one HLR (Walke, 2003). In addition, dynamic information about the mobile subscriber is stored, for instance the current location area (LA). A location area consists of one or a number of cells. As soon as mobile phone user leaves his current LA, this temporary data held in the HLR is immediately updated (Steele et al., 2001).

b) Visitor location register database (VLR)

The visitor location register (VLR) is a temporary database that maintains information about subscribers that are currently physically in the region covered by the mobile switching centre (MSC). Entries are added when visitors enter the VLR domain and deleted when visitors leave the VLR's domain.

The VLR stores information transmitted by the HLR, such as authentication data, telephone number, agreed services, allowing the MSC to make a connection. It temporarily stores a user's last known location area and records whether or not the subscriber is active and other parameters associated with the subscriber. The VLR also contains information that enables the network to find a particular subscriber in the event of an incoming call.

c) Authentication centre database (AuC)

The authentication centre database (AuC) handles authentication and encryption keys for all subscribers in the home and visitor location registers. It stores data needed to authenticate a call and to encrypt both voice and data traffic.

d) Equipment identity register database (EIR)

The Equipment identity register database (EIR) lists stolen phones, stores subscriber and equipment numbers (IMEI) of phones that are to be banned from the network or to be monitored. It can block calls from stolen mobile stations and prevent network use by handsets that have not been approved (Walke, 2003).

2.1.2.2 Steps in making a mobile phone call

To demonstrate how the cellular architecture works, described below is what happens when a call takes place between two mobile users within an area controlled by the same mobile switching centre (MSC) (after Stallings, 2005; Walters and Kritzinger, 2000).

Step 1: A mobile unit is turned on - initialisation

The mobile phone scans and selects the strongest setup control channel. The mobile phone selects the base station antenna of the cell within which it will operate, which must not always be the geographically closest base station due to interference patterns or other electromagnetic phenomena. A so-called handshake takes place between mobile phone handset and the mobile switching centre through the base station, which is used to identify the mobile phone user and to register its location. As long as the mobile phone is switched on, this scanning procedure is repeated frequently and if the phone enters a new cell, a new base station is selected.

Step 2: Call origination - request for connection

A mobile phone initiates a phone call by sending the number of the called mobile phone on the pre-selected setup control channel. The mobile phone's receiver first checks that the setup channel is idle by scanning the base station's forward control channel, also known as reverse control channel. When an idle is detected, the mobile is able to transmit on the corresponding reverse control channel to the base station, which then in turn sends the request to the MSC.

Step 3: Paging

The MSC completes the connection to the called mobile phone by sending a paging message to particular base stations depending on the called mobile number. Which base stations are paged depends on the mobile phone network provider but is also dependant on the physical position of the mobile phone. The mobile phone network is aware of the current position of a phone because it is stored in the VLR. Hence, only the relevant base station and those base stations in surrounding cells are addressed. Each BS transmits the paging signal on its own assigned setup channel.

Step 4: Call accepted

The called mobile phone recognises its number on the setup control channel it monitors frequently (see step 1). The mobile phone then responds to the relevant base station, which in turn sends the response to the MSC. The MSC sets up a

connection between the calling and called mobile phone. At the same time, the MSC selects an available traffic channel within each base station's cell and notifies each base station, which in turn notifies its mobile phones. The two mobile phones tune to the channels assigned by the base station.

2.1.3 Mobile location-based services (LBS)

“Location-based services are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device” (Virrantaus et al. 2001 in Steiniger et al., 2006). Location services are available to operators of all commonly used mobile phone networks in Europe: GSM (2G), GPRS (2.5) and UMTS (3G).
The value of knowing the location of a mobile phone handset has been acknowledged by private and public sector services. The geographic location of a mobile phone can either be used to enhance existing service applications or to create new ones. The following categories of location-based services (LBS) are commonly distinguished:

Safety and security

- Emergency services (Europe: E112, US: E911)
- Roadside assistance
- Child finder
- Asset tracking
- Employee safety
- Retention of traffic data, including location data in the EU

Social

- Games
- Friend finder
- Dating

Navigation and information services

- Traffic and weather reports
- Navigation information (Find the quickest route / Find my nearest …)
- Tourist services

Tracking services and logistical telematics

- Field Staff Management (Job scheduling)
- Fleet management
- Alerts on unauthorised locations

(Sources: Elliot and Phillips, 2004; m-location.com, n.d. ; Qualcomm, 2003)

These LBS typically use either active or passive location requests. The former are initiated by the mobile phone user, for example, when a mobile phone user wants to find the nearest bank. Passive location requests are not initiated by the mobile phone user and primarily encompass security and safety related applications, such as location tracking for emergency services and tracking of work force for business users.

Location-based services need to meet the expectations of subscribers and of mobile phone operators in terms of implementation and cost requirements. Performance requirements of LBS include consistency, start time and accuracy. The requirements for accuracy vary depending on the application - the majority of applications require accuracy of 10-100 metres range. Implementation requirements consider impacts on handsets, e.g. drain on batteries, roaming between networks (2G to 3G) and network expansions. Costs to take into account by operators include handset costs, infrastructure, expansion maintenance and return on investment (Qualcomm, 2003).

2.1.3.1 Location-enhanced emergency call services

In many emergencies people do not know their exact locations, which is particularly important when making the emergency call from a mobile phone. By using location-identifying technologies, emergency response times and thus consequences of injuries can be reduced. Around 180 million emergency calls are made in the European Union every year of which 60 to 70 percent originate from mobile phones. Possibilities for emergency call management are being investigated by European initiatives (European Commission, 2003). In the US, business drivers for location-based services include government mandates such as Enhanced 911 (E911) that require the incorporation of location-determination capabilities in mobile phones. The US's Federal Communication Commission (FCC) required US mobile phone service providers to provide public safety agencies with location information in the event of an emergency. Particular performance characteristics for location determination were specified (Centre for Democracy and Technology, 2006).

In Europe, calls made by mobile phone to '112', Europe's universal emergency number, will be able to inform the emergency services about the caller's location based on Cell-ID. Mobile phone service providers will share location information with the relevant emergency service. In Europe, opposed to the USA, no specific performance standards have been set for the member states.
Article 6 of the Directive on Universal Service and Users' Rights relating to Electronic Communications Networks and Services (2002/22/EC of 7 March 2002) states that:

"Member States shall ensure that undertakings which operate public telephone networks make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls to the single European emergency call number 112" (European Commission, 2002). This makes it a legal requirement for mobile phone service providers to deliver location enhanced 112 services across Europe.

In the EU, similar to the US and Canada, consumer consent for use of location data for emergency services is implied. The European Union has left it to voluntary efforts by industry to exploit the commercial capabilities of location-based services, however, has made it mandatory for mobile phone operators to pass on the location of callers as it is technically possible for them (Gow, 2004).

2.1.4 Different methods for locating a mobile phone

The various techniques for identifying the location of a device can be divided into network centric, handset centric methods or a combination of both. Network centric techniques locate a device based on information supplied by the network or with help of a number of mobile phone base stations, no handset enhancements are necessary. Handset centric methods require an upgrade to the mobile device as the location is calculated by the mobile phone itself from signals received from base stations. Satellite based technologies, such as GPS (see 2.1.4.2) are an example for handset- centric positioning (Steiniger, 2006).

The following location technologies are relevant to mobile phone location data and will be described together with their particular performance and implementation characteristics. Table 2.1, below, list the different methods.

Table 2.1: Mobile phone location technologies and supported mobile communication standard

Mobile phone location technology	Supported in mobile communication standard
Cell of origin (COO)	GSM, GPRS, and UMTS
AOA (Angle of Arrival)	GSM, GPRS
TDOA (Time Difference of Arrivals)	GSM, GPRS
E-OTD (Enhanced Observed Time Difference)	GSM and GPRS
OTDOA (Observed Time Difference of Arrival)	UMTS
A-GPS (Wireless Assisted GPS)	GSM, GPRS and UMTS

2.1.4.1 Network-based mobile phone positioning

Cell of origin (COO)

The simplest technique to identify the location of a mobile handset is based on cell-id, also known as Cell of origin (COO), see Figure 2.3. Since a mobile phone can be situated anywhere within a cell, the accuracy of these methods depends on cell size, which can vary from a few hundred metres to several kilometres (for more detail see section 2.1.2.1 above).

This method of locating a mobile phone is the least accurate but also the most inexpensive one, as it does not require individual handsets or network infrastructure to be altered. The location of the cell used by the mobile phone can be identified within about three seconds (Lyon, 2005). Accuracy of the Cell-ID method can be improved by specifying the cell sector, as each base station typically has multiple antennas, each covering a sector of the cell (see Figure 2.4). For example, a base station with three antennas will produce a cell with three 120 degree sectors. By detecting the antenna with which the handset registers, the location can be narrowed down to a sector of the cell (D'Roza and Bilchev, 2003).

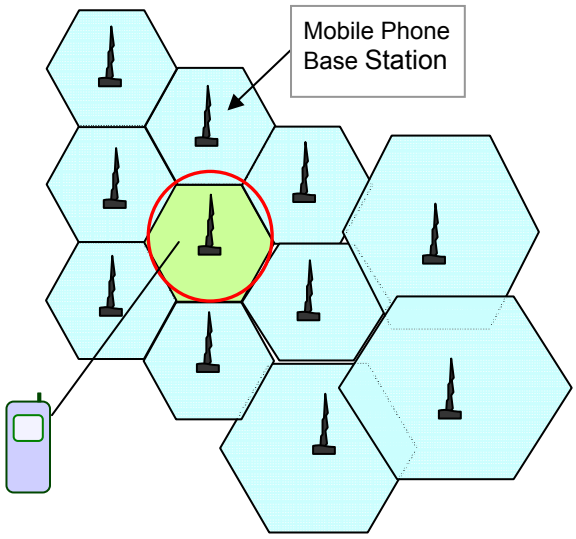


Figure 2.3: Cell-of-Origin tracking (after Walke, 1999)

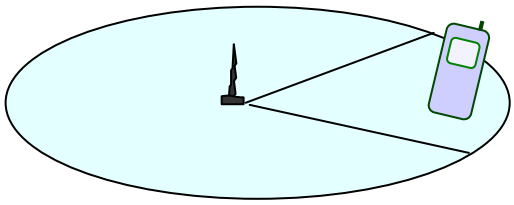


Figure 2.4: Sectorisation of a cell (after D'Roza and Bilchev, 2003)

Angle of Arrival (AOA)

A technique known as Angle of Arrival (AOA) determines a user's location by measuring the angles from which a mobile phone's signals are received by two or more base stations. Because the mobile device is moving, this is not a very exact method (Steiniger et al., 2006). The base stations need AOA equipment to identify the direction of the phone's signal. The AOA equipment compares the angle between the caller and various receiving base stations and uses triangulation to determine the caller's longitude and latitude. Limitations of the AOA technique include its reduced accuracy; for example when various forms of signal interference occur. This can be due to signals bouncing caused by high buildings, which results in a weaker signal or none at all. AOA is known to work best in less populated areas, as there is a lower likelihood of interference. Many companies combine AOA with TDOA according to Deitel et al. (2002). AOA is more accurate than COO and the handsets do not have to be modified. However, it can prove costly to modify and configure the base stations (Lyon, 2005).

Time Difference of Arrival (TDOA)

The Time Difference of Arrival (TDOA) technique measures the time it takes a mobile phone signal to reach the receiving tower and two additional towers. The signal's travel time allows determining the user's distance from each tower, which in turn allows calculating the user's position. By calculating the user's distance from the receiving tower and two adjacent towers, a (virtual) set of arcs is created, which intersection indicate the handset's location. Handsets do not need to be modified to utilise this location technique, as the calculation of the position is done by the network provider (Deitel et al., 2002).

Enhanced Observed Time Difference (E-OTD)

Enhanced Observed Time Difference (E-OTD), uses triangulation between at least three different base stations to provide more accurate location identification than Cell-ID. The distance between handset and base station is calculated based on the different times it takes a signal to arrive at the base stations once it leaves the handset. Accuracy can theoretically reach 30 metres but can lie in reality between 50 and 125 metres (Lyon, 2005).

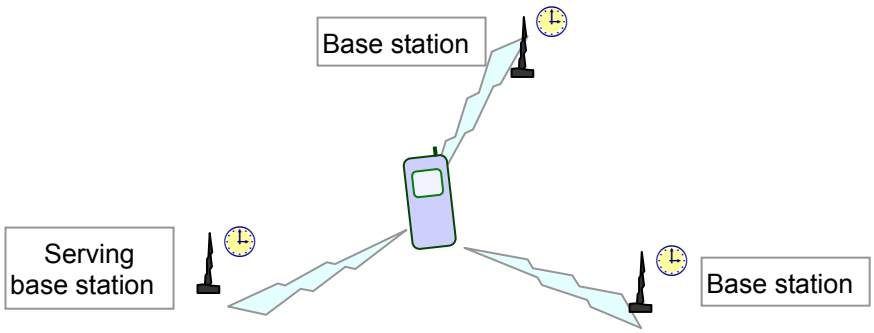


Figure 2.5: E-OTD (after Lyon, 2005)

E-OTD only works in GSM and GPRS networks, requires an upgrade to the mobile network infrastructure, and uploading of software to base stations to ensure compatibility. The base stations need to be fitted with location measurement units (LMUs) and, by measuring the signal from the mobile phone, the LMUs can triangulate the user's position. This technique offers greater accuracy than cell-of-origin but at a slower speed of response, typically around five seconds (Prasad, n.d.). Differing from TDOA, the calculation of the position is done by the mobile phone handset and for this reason a handset update in the form of software modification is necessary (Steiniger et al., 2006). A similar technique known as OTDOA (Observed Time Difference Of Arrival) operates only in 3G networks (Deitel et al., 2002).

2.1.4.2 Satellite-based mobile phone positioning

Global Positioning System (GPS)

The Global Positioning System (GPS) uses a set of satellites and ground receivers to determine the location of a GPS-enabled device. A GPS's receiver location is calculated by comparing time signals from several satellites, of which each has to have a direct line of sight to the receiver. At least three satellites are necessary to determine the receiver's two-dimensional location (i.e. latitude and longitude). To achieve additional and more accurate information, for example altitude, four or more satellite signals are required.

The 24 satellites orbit the earth twice a day, transmitting radio signals from approximately 12,000 miles above the Earth. The satellite system, based on spy satellites utilised during the Cold War, was originally developed by the USA Department of Defence to help troops and missiles locate themselves on maps. In the 1980s, the US government made the system available for civilian use. Once a GPS receiver has been acquired, the location identifying service is free to use and accurate to an average of 15 metres. However, the drawbacks for GPS receivers that have been integrated into mobile phone handsets are that GPS receivers consume a considerable amount of battery power, are fairly expensive, and location positioning does not tend to work from inside buildings as a direct line of sight with satellites is needed. In addition, in urban areas the GPS signal can bounce of building walls and distort the result (Monmonier, 2002; Lyon, 2005).

Assisted GPS

Assisted GPS (A-GPS) links to the terrestrial-based system of cell sites to speed up the process of calculating a handset's position. A-GPS can be combined with Cell-ID, E-OTD or OTDOA. It requires an update to the handset and network infrastructure and shares the same drawbacks as all GPS receivers (Lyon, 2005).

Galileo - European Satellite Navigation System

Galileo is a European satellite navigation system currently in development. It aims to provide positioning services from 2011 and to offer at least the same performances as GPS (European Commission, 2006b). Galileo's navigation infrastructure, which will consist of 30 satellites and relevant ground infrastructure, is funded by the European Union and the European Space Agency (European Commission, 2006a). Galileo is under civil control and aims to ensure that European economies are independent from other states' systems, such as GPS. GPS is a

military system by the United States and is made available to civil users without any guarantee for continuity.

Figure 2.6 below shows a comparison of the accuracy of positioning methods used by mobile phones:

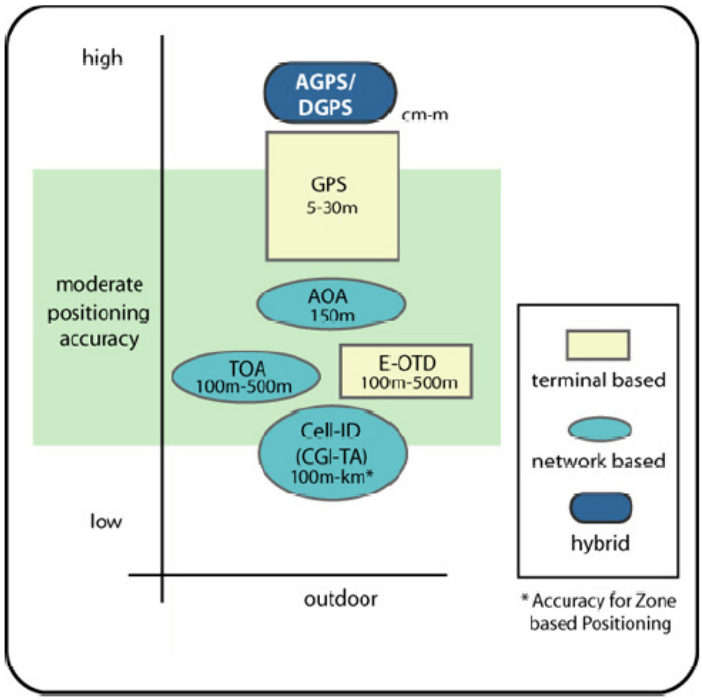


Figure 2.6: Accuracy of positioning methods (after Steiniger et al., 2006)

As can be seen from the graphic above (Figure 2.6), the most accurate ways of determining a mobile phone's geographical location involve the satellite based system GPS. Location identification by cell-ID is the least accurate method, however this technique makes use of the default properties of mobile phones. In other words, every mobile phone can be located by Cell-ID without any modifications of either software or hardware.

2.1.5 Summary Part 1

As can be seen from this short discussion of technical background, the location of every mobile phone can be identified by triangulating the mobile phone signal, irrespective of mobile phone network generation and network provider. This first part of the chapter has explained this process by providing an overview of the cellular GSM network architecture and techniques used for locating a mobile phone. Location information as part of other communications data can be stored for future data-mining and analysis, as for example for commercial location-based services or for law enforcement purposes, as discussed in Part 3 of this chapter (section 2.3). The automatic generation of digitised personal data about every mobile user and its storage on a long-term basis, may also bear negative aspects that can impact in individuals' privacy, as discussed in the next section.

2.2 Part 2: Privacy

The second part of this chapter focuses on the representation of privacy in the literature and starts off by introducing and classifying the wide range of privacy definitions. Following this, legal and technological matters relevant to privacy are reviewed together with issues of surveillance and social justice. In addition, this section addresses the role of privacy enhancing and invading technologies, and finally explores the relationship between location-based services and privacy in the literature.

2.2.1 Setting the scene

The difficulty of defining the concept of privacy is often used as an introduction to reviews of privacy literature (see for example Introna, 1997; Solove, 2002; Bennett, 2004). Alan Westin, a renowned US privacy scholar, comments on this subject matter that "no definition of privacy is possible because privacy issues are fundamentally matters of values, interests and power" (Westin, 1995, quoted in Gellman 1998, p. 194).). He suggests understanding privacy as an interest individuals have in leading a life free from interference by others. Despite this apparent slipperiness of the notion of privacy, numerous scholars have not ceased to provide their thoughts on this subject over the last several decades: such as regarding the impact of technologies on privacy (Cavoukian and Tapscott, 1995; Agre and Rotenberg, 1997; Bennett, 2004), surveillance and privacy (Clarke, 1988; Lyon, 1994; Zureik, 2005) or regarding communications interception in the information age (Diffie and Landau, 1998).

Fried (1968 in Singh and Hill, 2003) observes that privacy is of high value for people because it allows for transactions that result in trust, which otherwise without the reassurance of privacy would not be possible. Privacy is seen as an interest of the human personality and by some believed to be the most essential human right of the modern age (Privacy International, 2003b). Despite the apparent difficulties in finding a suitable characterisation of privacy, a right to privacy is enshrined in international treaties, conventions, and agreements. In 1948, the UN declared privacy to be a fundamental human right in Article 12 of the Universal Declaration of Human Rights (UDHR). The UDHR consists of 30 Articles which outline the United Nations General Assembly’s view on human rights guaranteed to all people. Yet, privacy was declared a *fundamental* right in the Universal Declaration of Human

Rights, differing from an *absolute* right, which is inviolable. Fundamental rights may under certain circumstances be removed (Gauntlett, 1999).

Shortly after the UDHR the Council of Europe released the European Convention on Human Rights, which states in its Article 8.1 that "Everyone has the right to respect for his private and family life, his home and his correspondence". It has been established under the jurisprudence of the European Court of Human Rights (ECtHR) (see for example Kopp v Switzerland (1999) 27 EHRR and Halford v United Kingdom (1997) 24 EHRR 523) that interception of post and telecommunications from business and private premises falls within the scope of Article 8.1 and therefore ensures private conversations to individuals (Davis, 2003). However, Article 8.2 ECHR allows interference with this right to respect for private and family if it is “necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (ECHR, Article 8.2) (for more detail see section 2.2.3.1).

Meanwhile, some philosophers believe that privacy rights are unequivocal and unconditional (McWhirther and Bible, 1992; Velasquez, 1992 in Singh, 2003). Goodwin (1991 in Singh, 2003) interprets privacy as a two-dimensional concept requiring space and information, whereas Gavison (1980) identifies the following three elements of privacy: secrecy, anonymity and solitude. Fried (1968) defines privacy as "control over knowledge about oneself", which corresponds to Westin's (1967, quoted in Garfinkel and Gene, 2002, p. 205) definition "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Westin supplies the following views of privacy,

a) Privacy as limited access to self, that is the extent to which we are known to others and the extent to which others have physical access to us

b) Privacy as control over information, that is not simply *limiting* what others know about you, but *controlling* it. This assumes individual autonomy in that one can control information in a meaningful way.

Privacy is again suggested to comprise the two factors control and knowledge by Foxman and Kilcoyne (1993 in Singh, 2003), in other words to have control over what information is collected and the knowledge that a data collection takes place

and including the purpose of collection. These definitions predominately relate to the categories of information privacy as discussed in the next section. Theoretical approaches to privacy predominantly differentiate between the following two aspects; protection of personal territory and protection against governmental intrusion. This relates to the traditionally recognised desire to balance the power between government and private individuals, as discussed by Nissenbaum (1998).

2.2.2 Privacy categories

The range of scholarly thoughts on privacy above indicates that there seems is no universally accepted definition of privacy. For these reasons, it seems the most useful approach to come to terms with the concept of privacy by applying different categories or spheres of privacy. All definitions of privacy supplied by the various authors above can be assigned to one or more of the following privacy categories.

The following four spheres of privacy are commonly identified (see for example Nissenbaum, 1998; Clarke, 1999; Gauntlett, 1999; Privacy International, 2003b):

a) Information privacy
b) Privacy of communications
c) Bodily privacy
d) Territorial privacy

In addition to these categories, Introna (1997) suggests the following three privacy categories, which share the element of 'personal information' as a common characteristic. These particularly relate to the empirical findings of this study, which will be discussed in detail in subsequent chapters:

e) privacy as no access to the person
f) privacy as control over personal information
g) privacy as freedom from judgement by others

These seven privacy categories as listed above are commonly referred to in the literature and are detailed in the following; the two categories relating to information (a+f) have been combined.
In the context of mobile phone location data and its long-term storage, the most obvious threat to privacy is towards the right to respect for private life as contained in Article 8 ECHR (see section 2.2.3.1). Information relating to an individual's geographical location and gathered on a continuous basis can be classified as privacy invasive according to six out of the following seven privacy categories:

a) Information privacy, f) Privacy as control over personal information

The categories of 'information privacy' and 'control over personal information' are the most frequently referred to privacy categories in the literature and are particularly relevant regarding modern information and communication technologies (ICTs). Mason (1986) identifies two forces related to information that threaten individual privacy. For one part the growth of information technology with its ability to generate, store and analyse great amounts of personal information, and for the other part the increased value of information in decision making to policy makers. The increased deployment of computers in the 1960s and 1970s has enabled businesses to store vast amounts of data at relative low cost for almost unlimited periods of time and has facilitated the linkage and analysis of data stored in different locations. These technical developments have resulted in the need of rules to manage the collection and handling of personal data, particularly consumer information (Privacy International, 2003b). In addition, the increased use of technology had already in the 1970s resulted in growing concerns about the potential of information technologies to accumulate detailed collections of information about individuals. Therefore the data protection legislation has been developed, in order to prevent harm to individuals and negative consequences on society. At first by some individual countries and then at international level, for example through the European Union. The UK's domestic version of data protection law was enacted in form of the Data Protection Act 1984. Today, the Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and Freedom of Information Act 2000 (Information Commissioner, 2007).

The predominant aim of most data depositories or data warehouses is to analyse the accumulated consumer data and detect patterns in order to identify consumer choices and preferences. Profiles of consumers groups are generated, supposedly facilitating the establishment of long-term relationships between business and consumer. A well-known and often cited principle in customer relationship marketing proclaims, "it costs six times more to sell to a new customer than to an existing one" (Kalakota and Robinson, 2001, p.170). In addition to these commercial uses of personal data generated by information and communications technologies, the data is used for law enforcement by the police and intelligence services. For example, the profiling of suspicious groups of citizens as part of a pro-active risk management by the government are matters that will be addressed later in this chapter (see section 2.2.5.2). Mobile phone location data is an example of personal information

specific to a mobile phone user and hence falls into this information privacy category. However, the mobile phone user does not have control over the generation of mobile phone location information or who has access to the data and for what purposes, which will discussed in further detail in subsequent sections.

b) Privacy of communications

The dimension of communications privacy deals with the claim of not being subjected to eavesdropping when communicating with others (Clarke, 1999a). This is also known as interception privacy. The European legal framework defines the right to communication privacy as fundamental and not as an absolute right, since court orders can be used to allow wiretapping (Gauntlett, 1999). However, it is widely agreed that wiretapping and electronic surveillance are highly intrusive forms of investigation that should be limited to exceptional circumstances (Privacy International, 2003b). Even though communications data does not encompass the content of communication, it nevertheless contains very personal information such as who has contacted whom, when, for how long and how often (see section 2.3.2).

c) Bodily privacy

The area of bodily privacy, also known as privacy of the person, is assigned to the matters of shielding one's physical self against procedures such as invasive body searches, genetic and drug testing. Person-identifying techniques based on physical and other characteristics, such as biometrics also fall into this category. However, mobile phone location data cannot be seen to be related to bodily privacy, as it contains information about a person's location and movements (see next privacy category).

d) Territorial privacy

This type of privacy deals with physical space and the protection of one's home or territory from direct intrusion. Territorial privacy also extends to the use of reasonable force to defend one's home against intruders (Gauntlett, 1999). The dimension of territorial privacy can also be categorised as media privacy, as it can also relate to behaviour in private and public places and visual surveillance, such as CCTV cameras. The standard of privacy protection regarding territorial and communication privacy was approved on international level in the UN Universal Declaration of Human Rights in 1948 (for more detail see section 2.2.3). The use of CCTV was regulated for the first time by the Data Protection Act 1998 to put the collection and storage of citizens' information to closer legal control (Moran, 2005).

Mobile phone location data encompasses information about the physical space that the mobile phone user accesses, which is then retained on a continuous and long-term basis under recent legislation (section 2.3.3.2).

e) Privacy as no access to the person

The privacy literature frequently refers to an article by Warren and Brandeis published in the Harvard Law Review from December 1890, in which the authors define personal privacy as the "right to be let alone" and "being free from intrusion" (Warren and Brandeis, 1890). However, this relatively early definition of privacy had not only related to the shielding of the home from intrusion but it was also a response to technology and market developments, i.e. the development of the camera and the emerging tabloid media. Warren and Brandeis' legal opinion tends to be presented as the initial one on privacy and still greatly influences today's privacy advocates. Mobile phone location data gives access to a person's location and communications habits and hence falls into this category of privacy.

g) Privacy as freedom from judgement by others

Johnson (1989 in Introna, 1997) describes privacy as a concept that varies from context to context and points out that “it is quite possible that no single example can be found of something which is considered private in every culture”. Privacy is here seen in the sense of a private space of immunity from the judgement of others, based on preconceived ideas and norms. In the case of mobile phone location data this may result in an individual being judged by others depending on where she or he has been. From historical information it may be deduced how this phone user may behave in the future.

To conclude, mobile phone location data can be seen as related to the majority of - six out of seven - commonly referred to privacy definitions. As will be discussed in further detail in subsequent sections (2.2.5), the long-term retention of mobile phone location data, together with other communications data, can be interpreted as a form of surveillance. Hence, in order for citizens to accept and to consent to this form of surveillance, it is necessary to ensure that governments are accountable for its actions (Taylor, 2002). The following sections will focus on the legislative framework for privacy and surveillance in relation to communications technologies.

2.2.3 Legal dimensions of privacy

A common misunderstanding between legal rights, on the one hand, and moral or natural rights, on the other hand, is highlighted by Clarke (1999a) and Langford (2000). Privacy is seen as equivalent to liberty and this definition confuses the legal right of privacy with the condition of privacy. The notions of legal matters and privacy are not easily separable perhaps because the concept of privacy is often merely considered in the context of *protection* of privacy and therefore closely related to the legal framework. It could even be understood, that the subject of privacy is only recognised when an intrusion of privacy occurs.

Four major models for privacy protection based on various international standards are identified by Privacy International (2003b) and Beresford (2005). Firstly, comprehensive laws that govern the collection, use and dissemination of personal information by both the government and private sector. For example, Europe has a comprehensive regulatory model with a public official in charge for enforcing data protection legislation. In the UK, the Office of the Information Commissioner is an independent public body established to enforce compliance with data protection legislation, such as the Data Protection Act 1998. Bennett (1995) has shown that countries that have established a data protection agency provide better privacy protection for their citizens. Secondly, sectoral laws regulating certain areas of privacy protection, for example financial or medical privacy. Thirdly, various forms of self-regulation in which industry adopts particular codes for self-control and engages in self-policing. However, Beresford (2005) remarks that industry-wide consensus does not necessarily result in satisfactory consumer privacy. The latter two privacy protection laws can be for example found the in the United States. Fourthly, technological self-help for consumers through methods such as encryption, various digital payment methods and anonymous remailers. Depending on their application, these models can be complementary or contradictory. Privacy International (2003b) believes that the joint use all of the models together provides the most effective privacy protection for citizens.

The terms 'human right' and 'civil liberty' are often used in conjunction with the term privacy. Stone (2004) explains that the phrase human right is commonly drawn on in an international context, such as by the Universal Declaration of Human Rights and the European Convention on Human Rights. The term civil liberty tends to be rather

used on the municipal level. However, Stone also acknowledges that the distinction between both terms can be blurred.

2.2.3.1 Protecting Human Rights

At the end of the 19th century, the American lawyers Warren and Brandeis have established the basis for privacy protection constituted in legislation (see section 2.2.2). In Europe, the right to privacy is a highly developed area of law, and after the Second World War Human Rights have been laid out in legislation, also in an attempt of the democratic states to distinguish themselves from the Eastern Bloc regimes (Bowden, 2003). All Member States of the Council of Europe have ratified the European Convention for the Protection of Human Rights and Fundamental Freedom, also known as the European Convention on Human Rights (ECHR), which was adopted in 1950. All Member States of the European Union (currently 27 members) are members of the Council of Europe (a larger body of 45+ member states), and are thus bound by the ECHR.

The Council of Europe established the European Court of Human Rights (ECtHR), based in Strasbourg, to ensure observance of the European Convention on Human Rights. An important element of this Convention system is that an individual, company or other organisation can bring a case against their own government claiming a violation against the Convention. The UK had been a signatory of the ECHR since 1950 and thus has bound itself to observe the judgement of the ECtHR. Therefore, when the European Court in Strasbourg decides that the UK has violated a right under the ECHR, the UK needs to amend its law, policy or practice so as to give effect to the judgment, while it has some discretion in doing so. Hence, the British courts are not bound to follow the Strasbourg view, which makes it possible for a “distinct British approach to human rights” to develop (Davis, 2003).

The jurisprudence of the European Court of Human Rights on privacy is more complex than that on other Convention rights, argue Whitty, Murphy and Livingstone (2001). The ECtHR looks at underlying values instead of artificially distinguishing private and public categories. The Court has adopted a definition of ‘private life’ that is more general than merely considering a person's intimate sphere of personal autonomy. For example, the ECtHR has considered worthy of respect a person's sense of self and well-being but also relationships within the wider society. Relevant cases that have been decided by the Court in Strasbourg involve personal

information on a card index (Amann v Switzerland (2000) 30 EHRR 843), private zones (in Niemietz v Germany (1992) 16 EHRR 97), respect for 'correspondence' which can involve an internal telephone system (Halford v UK (1997) 24 EHRR 523), telephone conversations (Malone v UK (1984) 7 EHRR 14) and letter and telephone communications (Hewitt and Harman v UK (1992) 14 EHRR 657) (Whitty, Murphy and Livingstone, 2001).

In the United Kingdom, the Human Rights Act made the European Convention on Human Rights part of British law and with it the right to privacy for the first time in British history. The HRA was introduced in 2000 and is only applicable to public authorities and private organisations acting as public authority. Despite these limitations, the HRA also affects the British law for all organisations and citizens as it contains a set of principles that need to be brought into court in order to be interpreted. However, even prior to the Human Rights Act 1998 coming into effect, the ECHR had already had an impact on the law of the UK when British judges sought compatibility with the Convention in their judgement (Davis, 2003).

In addition, changes to the British law became necessary due to adverse rulings from the court in Strasbourg, for example, relating to telephone tapping and surveillance in the well-documented cases of Malone v United Kingdom (1984) and Halford v United Kingdom (1997), as mentioned above. In the former case, Malone claimed that he had experienced an infringement by a public authority to his right to privacy. He alleged that he had been under police surveillance, his telephone had been tapped and phone calls metered. 'Metering' is the equivalent of retaining traffic data from landline telephones and postal communication and includes data, such as the numbers dialled, time and duration of calls, as well as the address on a postal communication (Bailey, Harris and Ormerod, 2001). However, Malone’s legal challenge was unsuccessful as there was no enforceable right to privacy in English law. The public telephone system was not considered a confidential network and hence the interception of communications did not involve the violation of any of the applicant’s rights. Finally in 1985, the European Court of Human Rights ruled that police interception of individuals' communications was a violation of Article 8 of the European Convention on Human Rights.

Subsequently, Malone’s case led to the ratification of the Interception of Communications Act 1985 to comply with the Strasbourg judgement in Malone v UK (1984) but also with the privatisation of the telecommunications service. The Court

ruled that the legal regulation of the circumstances of telephone interceptions was not expressed with sufficient clarity in the UK as required under Article 8.2 of the ECHR (Whitty, Murphy, and Livingstone, 2001; Taylor, 2002).

The case of Halford vs United Kingdom (1997) concerned a private telephone conversation using an internal office telephone system, between a police officer and her lawyer regarding a sexual discrimination complaint against her police force. The interception of this conversation by the police had been declared admissible under English law as the Interception of Communications Act 1985 (IOCA 1985) did not apply to private telephone systems, and there was no other UK law that regulated these types of systems. However, Halford took her case to the European Court of Human Rights, which ruled that an intrusion on such internal telephone systems did not comply with the requirements under Article 8.2.

The Regulation of Investigatory Powers Act 2000 was introduced partly to comply with Halford v UK (1997) concerning private telecommunications systems and other new communication technologies. Part 1 of RIPA supersedes the IOCA 1985 and extends the definition of interception to include most forms of electronic communications including email (Taylor, 2002) (see also section 2.3.3).

2.2.3.2 European data protection law

European laws aim to set a common standard across all member countries and have to take into account different cultures and laws regarding privacy protection. Nevertheless it needs to be pointed out that the impact of EU Directives is different in each country, and depends on the different mentalities of the different nations (Hosein, 2003).

In 1997, the Telecommunications Privacy Directive (97/66/EC) was introduced by the European Union to specifically regulate telecommunications systems, such as mobile networks, telephone and digital television. The Directive guaranteed 'a right to privacy' regarding telecommunications traffic of individuals. Opposing to current practices, access to billing data for marketing purposes was restricted, and data related to phone calls had to be deleted after the phone call terminated (section 2.3.4). Two years earlier, in 1995, the Data Protection Directive (95/46/EU) was introduced by the European Union to protect personal information to ensure the free flow of personal data within the EU and to harmonise privacy laws amongst its

member countries. This Directive established that personal data can only be collected with consent of the individual. The data should be processed fairly and lawfully for limited purposes and only retained for a limited period of time. Individuals should have the right to access data collected about them and to delete or change incorrect data. Some data is categorised as sensitive data, such as data relating to political opinions, religious or philosophical beliefs, trade union membership, and therefore cannot be processed without the individual's explicit consent. In spite of this, an individual's agreement is not required in exceptional cases of public interest, such as medical or scientific research, for which alternative protection mechanisms have been established (Bainbridge, 2004; Moran, 2005).

The Data Protection Directive is, amongst other Directives, implemented in all European Union member states along with local laws. To enforce compliance with the EU Directive, a Data Protection Authority has been established in each country, to ensure independence of the executive governmental branch to avoid political influence. In July 1998, the British Parliament approved the Data Protection Act (DPA) to implement the European Union Data Protection Directive in March 2000. The British handling of data collection and dissemination is regulated by the Data Protection Act (DPA, 1998) and the Freedom of Information Act (FOI Act, 2000). Both the DPA 1998 and the FOI Act 2000 reflect the development to put the collection and storage of citizens' information to closer legal control (Moran, 2005). For example, for the first time the DPA 1998 regulated the use of CCTV, a technology that was increasingly being used for surveillance. The DPA contains eight Principles that ensure adequate handling of personal data, which is data related to specific living individuals. However, information that is necessary for safeguarding national security is fully exempt from the Data Protection Principles (Davis, 2003).

The FOI Act imposes a duty on public authorities, such as government departments and councils, either to publish or disclose on demand information and documents in their possession. However, many categories of information and documents are exempted from this duty, for example if the information could be accessed by other means or other legislation. The FOI Act is evidence of a move towards greater openness and accountability, which serves the idea of citizenship, makes abuse of power clearer to citizens and aims to enable voters to make informed choices (Davis, 2003). Compliance with the Data Protection Act and Freedom of Information Act is promoted and enforced by the Office of the Information Commissioner (ICO).

The ICO is the UK's independent public body set up to protect personal information and promote public access to official information an independent agency (Information Commissioner's Office, n.d.).

Davies (1997) criticises that data protection acts are not concerned with the full range of privacy protection issues. He warns that the narrow scope of the acts can lead to serious limitations, as these laws are only information laws and protect data before the people. In other words, data protection acts are merely concerned with the way personal data is collected, stored and accessed but do not question the action of collecting data in the first place. British data protection laws react to complaints of non-compliance rather than to proactively examine whether organisations comply with the law. For these reasons, the awareness of individuals regarding privacy invasions is seen as crucial, as claimed by the Parliamentary Office of Science and Technology (2002), Cady and McGregor (2002) and Accenture (2003b).
Further details about the British legislation relevant to mobile phone location data are discussed later in this chapter in sections 2.3.2 and 2.3.3.2).

2.2.4 Impact of technologies on the concept of privacy

Particularly considerations about the influence of technology on privacy are of relevance to this study. When Warren and Brandeis' published their definition of privacy at the end of the 19th century, protection of privacy might have sufficiently consisted in shielding one's home from intrusion and not being watched or overheard by others. Even though their definition of privacy as related to the "the right to be left alone" is still frequently referred to today, others increasingly focus on technological influences on the concept of privacy.

Already two decades ago, Mason (1986) claimed that we live in at an information age, in an information society. Continuous advancements in information and communications technologies have resulted in faster computer processors, cheaper storage and growing use of networking technologies, such as the internet. One effect of this technological 'revolution' is the increased digitisation of data. It enables routine storage and analysis of personal data on great scale, such as for example when using credit cards, the internet or mobile phones. Consequently, the increased power of computers together with the advent of the internet have influenced numerous aspects of life and hence the concept of privacy.

A number of predominantly North American publications tend to merely relate privacy to electronic communications, and seem to be primarily concerned about the 'Death of privacy in the 21st century' caused by information and communication technologies (see for example Cavoukian and Tapscott, 1996; Gauntlet, 1999; Garfinkel, 2001; Cady and McGregor, 2002). However, their treatment of privacy provides a too narrow view of the subject matter. This highlights the importance of taking into account time and context of privacy publications, as well as country and regional specific regulatory approaches, in order to provide a sufficient understanding of the subject of privacy.

Before electronic means of data storage were widely used by businesses, data could often be found scattered over different places. The cumbersome and sometimes impossible retrieval of this data could act as a kind of privacy protection. When merging data from different sources over time privacy related issues arise especially when data that has been perceived as non-sensitive at time of disclosure is combined with other data (Nissenbaum, 1998). The analysis of consumers' purchasing habits is often accompanied by the creation of consumer profiles, which is another area frequently mentioned in the literature feared to invade individual's privacy (Cady, 2002; Graeff and Harmon, 2002). Consumer profiling evokes associations with racial or criminal profiling; taking into account that not only past actions can be analysed but also future consumer behaviour, which is often tried to be predicted and possibly influenced. This entails the danger shared with all types of profiling in that assumptions are made about a person which are not necessarily accurate or complete. Bowden (2003) warns that collections of consumer data often take place without the unambiguous consent of consumers, who may give their agreement at the very beginning of a business relation but then over time forget about it. This also raises issues regarding the ownership of personal data, particularly in sensitive areas such as health.

2.2.5 Surveillance society - Threats to privacy by digital data collections

The dictionary defines surveillance as “close observation, especially of a suspected spy or criminal” (The concise Oxford English dictionary, 2001). The French word surveillance means literally to “*watch over*, from sur- ‘*over’* + veiller ‘*watch’* from Latin vigilare keep watch, Origin: early 19th century.” However, 'to watch over' can be interpreted in two ways, which represent the two faces of surveillance: on the one hand, protection or care and on the other hand, control. Lyon (2001) argues that the worrisome and unsocial aspects of surveillance pay for mobility, convenience, speed, security and safety in modern life.

Several authors claim that today's Western society has turned into a surveillance society (see Lyon, 2001, Marx, 2002 and Stalder, 2002). However, these authors do not perceive surveillance in the context of totalitarian regimes or regarding a centralised Orwellian ‘Big Brother’ figure but rather as relating to the continuous gathering of information facilitated networked computer systems: "Everyday life is subject to monitoring, checking and scrutinising" (Lyon, 2001, p. 1). In Lyon’s view, all societies that depend on information and communications technologies for administrative and control processes can be described as surveillance societies. Indeed, the UK is the country with the most CCTV cameras in the Western world, according to the Human Rights organisation Liberty (n.d.). There are 4.2 million cameras in the UK, which means that there is one camera for every 14 British citizens, according to McCahill and Norris (2003 in Norris et al., 2004).

In its recent report commissioned for the UK Information Commissioner, the Surveillance Studies Network’s shares this broad definition of surveillance:

> “Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at **surveillance**.”
>
> (Surveillance Studies Network, 2006)

The report warns that the routine tracking and information gathering mechanisms of the surveillance society are often not obvious to citizens. This makes it particularly important to incorporate checks and safeguards when collecting data to ensure accountability.

Nevertheless, some authors such as Bennett (2005), challenge the view of defining electronic data collections as a form of surveillance. Bennett stresses that a

distinction needs to be made between capture and storage of personal information on the one side, and on the other side, data analysis and manipulation of those whose data has been collected. He bases these claims on a case study in which he examines his own data tracks generated as an airline passenger when travelling within his own country Canada and across the border to the US.

In his view, the collection and storage of his passenger data by the airlines and airports does not constitute surveillance, as there is no further analysis of that data from which decisions are made. He criticises the use of the term surveillance in this context, as he perceives surveillance as a too broad definition. Bennett suggests using another concept or term to explain the practice of humans to monitor data in order to make decisions about individuals. He believes that identifying these practices as surveillance trivialises the real surveillance, for which he gives as an example the special attention to passengers with ‘risky’ surnames. In this context, it could be seen as more suitable to use the term dataveillance, which Clarke (1988) has introduced almost two decades ago to describe the systematic monitoring of people’s actions or communications through information technology. Nonetheless, whether the term 'surveillance' is used or not, the extensive collection of individuals data is seen with unease by privacy scholars.

2.2.5.1 Digital technologies changing the concept of surveillance: new versus traditional surveillance

The traditional definition of surveillance as close observation of a suspect individual with the naked eye does not necessarily apply any longer, due to the capabilities of modern technologies to routinely record data. Several authors such as Lyon (1994), Marx (2002) and Clarke (2005), agree that the concept of surveillance has changed over the last decades and have declared the emergence of “new surveillance”. Marx (2002) identifies 28 dimensions in which traditional and new surveillance differ. For instance, Marx describes the differences between ‘new’ and ‘traditional’ surveillance as concerning the collection of data. The generation of predominantly digital data in private life and commercial settings leads to fewer costs of data handling. Data collections tend to occur on a continuous and routine basis, which makes the gathering less visible and enables real-time availability of information, such as for example CCTV data, use of credit cards and mobile phones. Inexpensive storage space enables the long-term retention of data. In addition, faster computer processors make it easier to organise, store, retrieve and analyse data and help to

make predictions for the future. This can be relevant for commercial companies for marketing their products, as well as for governments in order to increase accuracy of planning as suggested by Stalder (2002). However, it seems that Marx solely bases his distinction of the differences regarding the two types of surveillance on the capabilities of modern ICTs, such as assistance with the handling of great amounts of data, or in other words on the continuing development of the technological age.

Marx (2002) places the emphasis of new surveillance on mass surveillance of groups consisting of anonymous individuals, rather than on the visible and noticeable monitoring of individuals. In addition, the increased storage and analysis capabilities enable a closer examination of certain subjects of surveillance, in real-time but also in retrospective. Lyon (1994) points out that it is not necessary to identify individuals in order to conduct profiling of behaviour and habits in relation to social demographics. He fears that this can lead to social sorting and demographic discrimination of groups of individuals. Davies shares Lyon's view and offers as an example the use of statistics by the British government, instead of suspicion, to justify the use of a range of new powers, such as DNA test and finger printing (Talk Simon Davies at Leeds Metropolitan University, 28th October 2005).

Different phases in the application of surveillance technologies are distinguished by Kim (2004). Firstly, physical surveillance, as described by Bentham (1791) and Foucault (1975), as for example by their ideas about the Panopticon; secondly the concept of electronic surveillance that places the emphasis on the use of technologies to expand the observing electronic gaze from prison or factory to the wider society with help of information technologies as discussed by Marx (1985) or Lyon (1994). Thirdly, data surveillance, also known as ‘dataveillance’ which is described as the systematic use of personal data systems in monitoring of the actions or communications of one or more persons by Clarke (1994b). As last phase of the social effects of surveillance technology, Kim (2004) introduces the notion of ‘hyper-surveillance’ and refers to the authors Bogard (1996) and Haggerty and Ericson (2000). However, the author fails to explicate the difference between the phases of dataveillance and hyper-surveillance, which seems to be minuscule.

Today's immense data collections are performed by a number of different agents. This contradicts visions of surveillance related to Big Brother, as described in Orwell's novel 'Nineteen eighty-four', or in other words *one* single data collection agency. Different data collection agencies can encompass commercial companies logging consumers' shopping or financial data, governmental agencies that record images of pedestrians crossing the streets, and interceptions of communication for keywords indicating terrorist activities by listening stations such as Menwith Hill in Yorkshire.

Some perceive a change in the privacy debate in that citizens used to be worried about either commercial companies *or* the government having access to their data. Even though neither of these concerns have vanished, there are now relationships springing up between commercial companies and the government (13th Annual Conference on Computers, Freedom & Privacy, Plenary Session #9: Data Retention in Europe and America, 2003). This collaboration between public and private sector actors particularly applies to the discussion about data retention. The government gains access to user's mobile phone communications data via privatised, commercial mobile phone and internet service providers.

2.2.5.2 Data shadows of individuals and implications of 'dataveillance' for society

The dangers and benefits of surveillance are identified most concisely by Clarke (1998) and Lyon (2001). Lyon believes that society profits of surveillance in terms of efficiency, mobility, security and public order. Clarke predominantly identifies the advantages of physical security and the data matching practices of organisations to combat fraud. Both authors point out as potential dangers of dataveillance the unintended consequences and negative dimensions of surveillance.

The threats of mass dataveillance can be divided into dangers to individuals and to society. Clarke (1998) identifies as dangers of dataveillance for individuals that decisions based on incorrect data may lead to unfairness. This can particularly become a problem when an individual is unaware of the data collection and hence has no means to rectify wrong data. Consequently, this can result in blacklisting a person over a matter that is still under dispute or falsely related to that person. Metaphors such as 'data shadow', 'data trail' or 'digital personae' are frequently applied in the literature to depict the effects of dataveillance on individuals (see for example Clarke, 1994b; Lyon 2001; Stalder 2002; Bennett 2005). The 'data shadow' is made up of personal data and follows or precedes an individual. The danger here

is the potential judging and discrimination based on data that might not be accurate. Nissenbaum (1998) points out that even though those who are aware of collections of their data may be less easily targeted or manipulated. Nevertheless, the awareness of data collection can create a climate of self-consciousness and suspicion. Clarke (2000) further perceives as a danger of surveillance that it makes it possible for authorities to focus on undesirable classes of people before they commit an offence. For example, the 1984 Police and Criminal Evidence Act gives police the right to stop and search on grounds of suspicion. This situation results in an inversion of burden of proof from the accusing organisation to the individual who now needs to provide evidence of their innocence.

Collections of personal data may not only be interpreted as a threat to personal privacy but more importantly as a danger to social justice. Clarke (1998) warns that "dataveillance is by its very nature, intrusive and threatening". Dangers of mass dataveillance to society can once again be described as to create a climate of suspicion, particularly when individuals are aware of the data collection, as well as decreased respect for the law and law enforcers, deteriorating of society's moral fibre and solidarity. The STOA report (European Commission's Science and Technology Options Assessment office) cautions of the surveillance capability of ICTs that may be used to track the activities of journalists, campaigners and human rights activists (STOA report, 1998). These technologies can result in a chilling effect on those who participate in democratic protest warns Privacy International (1999). Along the same lines Clarke (2005) indicates that privacy is important from a political viewpoint, enabling freedom of speech to think and act. In his view, the monitoring of individuals' communications and actions threatens democracy. Lyon (2003) argues that concerns about surveillance used to be expressed in terms of privacy and freedom. He warns that the digital divide is not just a matter of access to information but that information itself can be a means of creating divisions. Hence, personal data and communications data retention cannot merely regarded as an individual privacy concern but need to be framed as bearing an effect on society as a whole.

Already in his 1988 paper, Clarke identifies costs of collecting, storing and analysing data as a 'natural control' to limit dataveillance. However today almost 20 years on, this reason does not ring true anymore. As a result of most data being generated in digital format, the costs of automatic data collections and their analysis have decreased significantly. Clarke highlights the moral obligations of IT professionals,

marketers and governments in creating and using computer systems to handle individuals' data in an ethical way.

2.2.6 Privacy enhancing and invading technologies

The question whether technology itself can be seen as 'neutral', 'good' or 'bad' is frequently addressed by scholars (Clarke, 1999b; Cady, 2002). "There is nothing inherently good or bad about the increased power of technology" maintains Marx (2006, p. 38), and suggests that new technologies with privacy invasive potential must be subjected to empirical and ethical questions and not simply accepted as good because they are novel. In the same manner, Lyon (2002) argues that new information and communications technologies do not by themselves create surveillance but rather the application of technology and the policies accompanying its usage. May (2002) asserts that ICTs do not fundamentally change society and do not constitute an information '*revolution'* that requires entirely new thinking. Even though the author admits that technology has social, political and economic effects and transforms some activities within society, he also argues that this does not alter society's substance. In addition, he challenges the widely accepted view that the arrival of the 'information society' has fundamentally transformed society.

Some place technologies into categories according to their ability to invade or protect individual privacy (Clarke, 1999; Bowden, 2003). Data warehousing and data mining, as introduced in previous sections, are often perceived as predominantly privacy invasive technologies (PITs). To this category are also often counted authentication technologies such as biometrics and technologies, as they do not allow the anonymisation of data. Technologies that can be used to protect the privacy of users are known as privacy enhancing technologies (PETs). They protect the privacy of individuals and provide anonymity in transactions or provide a pseudonym. Examples of PETs are anonymous web browsers, remailers and encryption (Agre, 1997; Clarke, 1999, 2001). These PETs are an important part of the privacy model of technological self-help as introduced in section 2.2.3. Kim (2004) claims that PETs may help transparency as well as reconstruct interpersonal trust in the networked environment and can help the promotion and protection of privacy rights. However, the author also admits that PETs fail to acknowledge the drive (or motivation) for exploitation or dominance.

2.2.7 Mobile phone location data and privacy

It can be argued that location technologies pose new challenges for privacy policy and law. As explained above, location data has the potential to be used to create profiles, social sorting, discrimination and differential treatment, which often remain invisible to most members of the public (see Clarke, 2000; Lyon 2005; Surveillance Studies Network, 2006). Despite these claims, it needs to be clarified that a mobile phone's location may or may not correspond to the whereabouts of an individual presumed to be the user.

Mobile phones have always been 'location-aware', because location awareness is an inherent feature of mobile telephony as discussed in the previous part of this chapter (see for example section 2.1.2). However, in recent years the accuracy with which mobile phones can be located has improved, as well as the ability to store and process large amounts of data. It is now possible to preserve and access present and past movements of all mobile phone users over prolonged periods of time. As discussed in previous sections, British citizens are ensured a right to privacy under the European Convention on Human Rights, which as been brought into the domestic context by the Human Rights Act 1998. However, this right to privacy can be interfered with under a range of exclusive purposes listed in Article 8.2 ECHR (see previous section 2.2.1) and in accordance to the ECtHR's jurisprudence . Some have argued that the blanket retention of all citizens' communications data violates those rights to privacy and details will be provided in the subsequent section 2.3.3.2. Regarding the privacy categories commonly identified in the literature, it can be argued that location data falls into six out of the seven categories (see section 2.2.2). Only the category of bodily privacy, which relates to a person's physical self, cannot be seen as directly affected by location data. Particularly in the area of information privacy, which is concerned with individuals' personal data, a distinction needs to be made between the use of data for law enforcement and for commercial purposes. The use of communications data for the former falls under state surveillance techniques and is regulated by legislation such as the Regulation of Investigatory Powers Act 2000 (section 2.3.3.2).

The use of communications data for commercial services is for example regulated by the European Union Privacy Directive (Directive 2002/58/EC) and Vodafone's Code of Practice that regulate the access to location data (Vodafone's Code of

Practice, 2005). The Directive explicitly covers unsolicited messages for marketing purposes and stresses the need for prior consent (Article 13). Article 9 of the Directive deals with the use of location data and requires that location data may only be processed when made anonymous or with the consent of the user. Vodafone's Code of Practice (2005) distinguishes two types of location services, active and passive (see section 2.1.3), and stresses that particularly the latter require the informed consent of the mobile phone user. Gow (2004) stresses the role of consent as establishing the legal grounds regarding location data and its importance for understanding location privacy issues in the commercial context. He distinguishes between three moments of consent: collection, use and disclosure of personal data. In the same manner, White (2003) refers to three processes to identify privacy issues particular relevant to location techniques; firstly location identification, secondly data processing and thirdly value-added use. Spiekermann (2004) predominantly perceives unsolicited messages ('mobile spam') as privacy intrusions and points out that the mobile phone is a more personal device than for example a desktop PC.

To summarise, the authors highlight that the informed consent of mobile phone users is required to use mobile phone location data for commercial purposes. However, for the use of location data by governmental agencies, such as for crime and terrorism, the consent of mobile phone users is not explicitly obtained but acquired by the signature in the mobile phone contract. Further discussion of this matter will be provided in the next section.

2.2.8 Summary Part 2

As can be seen from the first part of this chapter, the continuous generation and long-term storage of digitised personal data is an inherent part of today's networked information and communication technologies. This second part has discussed the relationship and impacts of these technologies on individual's privacy. In addition to this, a range of privacy definitions were introduced and categorised according to several criteria. Current legislation relevant to mobile phone communications data and privacy were presented, while the use of location data for law enforcement and commercial use was differentiated. It has become clear that privacy is a concept that is hard to define and this is reflected in the jurisprudence of the European Court in Strasbourg, which decides on infringements of human rights, including privacy, on a case by case basis.

The following section offers an introduction to the legislative framework regarding the retention and access of communications data by law enforcement agencies, as relevant in the European Union with focus on the UK.

2.3 Part 3: Legal framework relevant to mobile phone location data

This final section of the chapter provides an insight into the legal framework relevant to mobile phone communications data. Firstly, the section provides some definitions for mobile phone communications data, of which location data is one element. The subsequent sections review the legislation and context up to and beyond the 9/11 terrorist attacks in the US, and as relevant to the retention of mobile phone communications data in England. The main two British legal instruments that is the Regulation of Investigatory Powers Act 2000 (RIP Act) and the Anti-Terrorism Crime and Security Act 2001 (ATCS Act) are discussed, as well as the European Data Retention Directive 2006/24/EC. Finally, the predominant arguments in the disputes and debates about the compulsory storage of all British' and also European mobile phone users' communications data are presented.

2.3.1 Definitions of mobile phone communications data

While Part 1 of this chapter (see section 2.1) has already provided some technical background to mobile phone location data, this section focuses on the legal definitions of communications data of which mobile phone location data is one element. The ATCS Act refers to the RIP Act for definitions of communications data to be retained by mobile phone and internet service providers. Communications data is defined under the RIP Act (section 21, 4 a, b, c) as follows:

Table 2.2: Definition of communications data (RIP Act, sect. 21, 4 a b c)

(4) "Communications data" means any of the following-

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

The 'Consultation paper on a code of practice for voluntary retention of communications data' (Home Office, 2003b, section 15) explains that communications data can be divided into three broad categories, such as:

- **Traffic data** identifies who the user contacted, at what time the contact was made, the location of the person contacted and **the location of the user**.
- **Service use information** are for example itemised telephone call records, i.e. the numbers called from a mobile phone, including times and duration.
- **Subscriber data** identifies the user of the service, providing their name, address, telephone number.

Appendix A of the consultation paper provides further details about data types retained and their retention periods, that is for example:

Subscriber information relating to the person encompass for example, name, date of birth, installation and billing address and payment methods.

Telephony data includes amongst other data,
- all numbers (or other identifiers e.g. name@bt) associated with call (e.g. physical/presentational/network assigned CLI, IMSI, IMEI, exchange/divert numbers) (for details about these see section 2.1.2.1 and glossary)
- Date and time of start of call, duration of call/date and time of end of call
- **Location data at start and/or end of call, in form of lat/long reference.**
- Cell site data from time cell ceases to be used.

SMS and MMS data include for example
- Calling and called number, IMEI
- Date and time of sending
- Location data when messages sent and received, in form of lat/long reference.

Subscriber information and telephony data are stored for 12months, whereas SMS and MMS data is only stored for 6 months.

To summarise, the British legislation defines mobile phone location data as an element of traffic data, which is one of the three categories of communications data. The European Directive on Privacy and Electronic Communications (Directive 2002/58/EC, Article 2, c) defines location data as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service". This Article applies to computers, PDAs and mobile as well as landline telephones. This Directive was more comprehensive than previous rules as it used the term 'electronic communications', instead of being restrictive to certain technologies.

The Directive 2002/58/EC was amended by Directive 2006/24/EC regarding the purposes for which the data can be retained by the service providers (see section 2.3.4). The 2002 Directive (section 14) further specifies that "Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded".

Hosein and Escudero-Pascual (2002) argue that new legislation concerning traffic data tends to be technology-neutral which does not take into account the differences in traffic data across different communications infrastructures and protocols. The authors point towards the differing definitions of traffic data from the Council of Europe (CoE) and the Group of eight industrialised countries (G8). Both definitions explain that traffic data "does not include" (G8, see Statewatch, 2001) or "does not refer to" (Council of Europe, 2001) content, however, Hosein and Escudero-Pascual (2002) point out that there are ambiguities particularly regarding internet data. For instance, click stream information of internet access logs closely relates to the content of everything that has been accessed and downloaded (Walker and Akdeniz, 2003). For example, within a communication, data identifying www.homeoffice.gov.uk would be traffic data, whereas data identifying www.homeoffice.gov.uk/kbsearch?qt=ripa+traffic=data would be content (Home Office, 2003a, page 7; Escudero-Pascual and Hosein, 2004).

As highlighted in the previous section 2.2.7, communications data is of relevance for commercial but also for law enforcement use. In this context, Green and Smith (2004) point out that different actors use differing interpretations of mobile phone location data, particularly regarding the relationship between mobile device and the individual associated with this device. On the one hand, location data is described as being connected to particular individual consumers and hence has economic value. It is for example used for mobile location-based services (see section 2.1.3), however only with the explicit consent of the mobile phone user (see section 2.2.7). On the other hand, industry sources and regulatory bodies claim that location data, as part of traffic data is anonymous and not connected to a specific individual. Green and Smith base this claim on one of their own case studies which highlighted the difference between billing data and traffic data. The former is personal, as it includes information such as the subscriber's name and address, and therefore needs to be regulated under the Data Protection Act. The latter is anonymised at

the end of the phone call but archived by the unique phone number and therefore still of commercial value to the telecommunications companies, according to Green (2006).
Nonetheless, it can be argued that even though an individual can hardly be identified solely by the mobile phone location data of his or her phone, the *combination of location data with other data* may constitute an infringement on a mobile phone user's privacy.

Mobile phone location data discloses location at the beginning and end of the call and hence records changes in location. The following shows an example of outgoing mobile phone call records:

Data Outgoing (Including Voice/SMS & Video Calls) for 078***975 for the period of 01/10/04 - 08/12/04**

Date & Time Of Call	Calling MSISDN	Called MSISDN	37 = Video Call	If populated with SMSC details then denotes SMS message)	Record Type	Duration In Seconds
19/11/2004 11:10	78*****975	**********			Mobile Originated	21
19/11/2004 11:11	78*****975	**********			Mobile Originated	3
19/11/2004 11:12	78*****975	**********			Mobile Originated	147
19/11/2004 11:39	78*****975	**********			Unsuccessful Call Attempt	

Figure 2.7: Example of a telecommunications call data record (UK Presidency of European Union, 2005, p.8)

2.3.2 Background to communications data retention

Communications technologies, such as the internet and mobile phones, are an inherent part of daily lives for the majority of European citizens. Every communication facilitated by such technologies generates a host of data, such as the source, destination, mobile phone location and partial web browsing logs. The data is stored for billing and legal purposes by mobile phone and internet service providers, which are, in the following, referred to as communications service providers (CSPs). This data about communication is also known as communications or transactional data. Since in western European societies citizens but also criminals increasingly use electronic communications and rely on technological infrastructure, the focus of legislators has turned to communications data in response to the September 11 US attacks. Attacks on the communications infrastructure are also included in the definition of 'terrorism' (Terrorism Act 2000, (2)) (Walker and Akdeniz, 2003).

Particularly, the process of adopting European Directives relating to communications data retention (2002/58/EC, 2006/24/EC) highlights the political climate change following the September 11 attacks (see section 2.3.4). Communications data is seen by security, intelligence and law enforcement agencies as a useful tool to prevent and investigate crimes related to national security. It is important to recognise that communications data does *not include the content* but instead only refers to information *about a communication*. The retained communications data can be analysed and helps investigators to identify suspects, relationships between them and to establish profiles. The Home Office, the ministry responsible for justice and internal affairs in the UK, points out that evidence from use of telecommunications can be the only physical evidence available to investigators (Home Office, 2003b, section 5). The rapidly changing technological environment and the requirements of law enforcement agencies to access the data while ensuring human rights of those affected by the legislation, poses challenges in legislating the area of communications data retention.

Historically, the content of communication has been perceived as more sensitive and personal than data about communication. Therefore greater authorisation and oversight mechanisms are still needed to gain access to the contents of communication (Escudero-Pascual and Hosein, 2004). However as Privacy International (2003b) points out, the sensitive nature of transactional data of new technologies makes it similar to content of communication. Data generated by an internet user's transactions convey a great deal about this person, because a profile of interests, associates and social context can be constructed. Similarly, location information included in mobile phone communication data is more sensitive than the location information of traditional fixed telephony communication.
Hence, the long-term retention of mobile phone communications data can be seen to affect a wide variety of human rights, including the right of freedom of speech and assembly, as well as the right to privacy. Considering the jurisprudence of the European Court of Human Rights in Strasbourg, the long-term retention of mobile phone communications data may be seen as a disproportionate interference in the private lives of citizens, and in turn the interference is not necessary in a democratic society (see section 2.2.3.1).

Digitisation and privatisation

With the invention of the microprocessor in the 1970s and with it the widespread use of personal computers, the processing power and storage capacity of computers has dramatically increased. The change from analogous to digital communications infrastructures makes it easier to store, gain access to and search transactional data. Difficulties of retrieving analogous transactional data had acted as a natural protection against unsolicited and excessive access and misuse of data. In addition, transactional data from analogous systems does not carry as much information as digital data carries today.

In 1981, the British Telecommunications Act transferred the responsibility for telecommunications away from the Post Office, creating a separate organisation, British Telecom (BT). At this time competition was introduced into the UK telecommunications industry. In 1984, the Telecommunications Act 1984 was passed and BT was privatised and thus lost its monopoly in running telecommunications systems. This was the first of a series of privatisations of state-owned utilities throughout the 1980s and into the 1990s (Daβler et al., 2002). This privatisation process has resulted in a situation where law enforcement agencies needed to approach businesses and not state owned companies for transactional data. In addition, changes in business models such as "always on internet access" and flat rates for internet and mobile phone use, have made itemised billing largely unnecessary. Hence communications service providers only store detailed data about mobile phone and internet usage for billing purposes for a limited time. These changes, away from state owned telecommunications business to private companies, made it more difficult for governmental agencies to access the communications data, hence, the introduction of new laws became necessary (Walker and Akdeniz, 2003).

As new telecommunications technologies emerge, many countries adapt their existing surveillance laws and for example, the case law in Strasbourg has been used to update existing British legislation to take into account new technological developments (see section 2.3.2). However, often governments apply old legislative instruments to new technologies to address the interception of networked and mobile communications without analysing how the technology has changed the nature and sensitivity of information (Privacy International, 2003b; Who Knows Where You've been? Privacy Concerns Regarding The Use of Cellular Phones As Personal Locators, 2004). Changes in legislation were the most obvious and

immediate responses in Europe to the terrorist threats by the 2001 attacks in the US. Security and law enforcement agencies worldwide have encouraged their governments to adopt more comprehensive approaches to the retention and access of communications data (Blakeney, 2007). This may explain why much research regarding communications data retention has focused on these legislative changes (see for example Walker and Akdeniz, 2003; Escudero-Pascual and Hosein, 2004; Whitley and Hosein, 2005).

2.3.3 Legislative developments regarding communications data in the UK

In the United Kingdom, two pieces of legislation are particularly relevant regarding communications data: the Regulation of Investigatory Powers Act 2000 (RIP Act), which regulates the *access* to communications data, and the Anti-Terrorism Crime and Security Act 2001 (ATCS Act), which lays down rules for the *retention* of communication data. The European Directive on Data Retention (2006/24/EC) also has an influence on the data retention regime in the UK, as it lays down requirements for the retention of communications data for all European member states.

The value of interception of communications for law enforcement agencies and its role to fight terrorism of all kinds has long been recognised by the British government. Already the 1999 Home Office Consultation paper 'Interception of Communications in the United Kingdom' proposed and justifies changes to the interception regime by law enforcement agencies at the time (Home Office, 1999). In this consultation paper the Home Office admitted that legislation had not kept up with changes in the telecommunications and postal market. For example, the number of telecommunications companies offering fixed line services had grown from 2 to around 150, and there was the beginning of mass ownership of mobile phones, as well as citizens embracing communicating via the internet. Together with this increase in electronic communication, the threat of cyber crime emerged, which is defined as criminal acts using technology or action against technology. Hence interception was thought to play an important role in law enforcement (Akdeniz, Taylor and Walker, 2001). Consequently, these technological developments made a more comprehensive legislative approach more desirable.

The Consultation paper 1999 proposed to establish a clear, statutory framework for access to communications data and this has resulted in the introduction of the RIP Act. Part 1 of RIPA addresses those proposed amendments regarding interception

of communications, also in response to rulings from ECtHR in Strasbourg where the case of Halford v UK has been particularly relevant (see section 2.2.1). In this case, the UK legislation at the time in form of the Interception of Communications Act 1985 did not extend to non-public telephone networks and hence this form of interception could not be carried out in accordance with the law.

2.3.3.1 Regulation of Investigatory Powers Act 2000 (RIP Act)

The RIP Act 2000 is the latest step towards the development of an inclusive code of policing and surveillance, including the surveillance of internet data. As described in the previous section, the increased use of mobile phones and internet by citizens, as well as rulings from the European Court of Human Rights in Strasbourg made a more comprehensive approach necessary (Akdeniz, Taylor and Walker, 2001; Bailey, Harris and Ormerod, 2001). The RIP Act also sought to regulate surveillance of the types of communication not dealt with in the Police Act 1997, as for example pagers, mobile phones or emails. The Act extends the legislative powers in relation to post and telecommunications surveillance by replacing the Interception of Communications Act 1985, which it repealed. The Interception of Communications Act 1985 permitted law enforcement agencies to have access to communications, which later had to be limited under the Human Rights Act 1998 (Hosein and Whitley, 2002). Prior to the 1985 Act, the interception of communications was not regulated by statute but by Home Office administrative practice that was given implicit recognition by the Post Office Act 1969, s. 80. (Bailey, Harris and Ormerod, 2001).

The Regulation of Investigatory Powers Bill was introduced to the House of Commons on February 9th 2000 and was given the Royal Assent, which means that it became law, on July 28th 2000. The RIP Act aimed to ensure compliance with the ECHR and the Human Rights Act 1998, as Secretary of State for the Home Department, Mr. Jack Straw, highlights in the RIP Bill's Second Reading in the House of Commons:

> "This is an important Bill, and represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting. None of the law enforcement activities specified in the Bill is new. What is new is that, for the first time**, the use of these techniques will be properly regulated by law and externally supervised**. That will serve to ensure that law enforcement and other operations are consistent with the duties imposed on public authorities by the European Convention on Human Rights and by the Human Rights Act 1998."
>
> (HC Debate, 2000, Column 767)

The RIP Act enables secret services to monitor all online activity in the fight against cyber crime. It allows senior members of the civilian and military police, customs and members of the judiciary to demand that users hand over the plaintext of encrypted material or in certain circumstances decryption keys themselves. Part I of Chapter II of the Act deals with acquisition and disclosure of communications data. The provisions of Chapter II came into force on 5th January 2004 (Home Office, 2000).

The RIP Act was highly contested when it was introduced into Parliament, as the viewpoints of government, industry and privacy advocates differed widely.
Issues of discussion were the development of legislative instruments in the face of continuously changing technological developments, meeting requirements of law enforcement agencies to access the data while at the same time maintaining the human rights of those affected by the legislation (Hosein and Whitley, 2002). After a public consultation in August 2001, controversies arose regarding surveillance concerns, as the RIP Act allowed the Home Secretary to designate a large number of public authorities to access communications data without a warrant.
In June 2002, David Blunkett, the home secretary at the time, suggested expanding the RIP Act greatly by extending the number of public bodies to 1039 public authorities to monitor citizens' communications data. The draft secondary legislation under section 25 RIP Act proposed allowing access to communications data without a warrant to Government departments, such as the Department for Environment, Food and Rural Affairs, and the Department of Health, as well as Local authorities and other bodies, such the Environment Agency and the Scottish Drug Enforcement Agency (The Regulation of Investigatory Powers, Communications Data: Additional Public Authorities Order, 2002).
This resulted in a controversy about the expansion of power and those plans became known as "Snoopers' charter" (BBC News, 2002). The Surveillance Commissioner admitted in his annual report that he could not ensure meaningful oversight of so many bodies without assistance. Following protests of civil liberties groups, the media and opposition in Parliament and from the Information Commissioner, the Statutory Order was withdrawn on 18 June 2002 (Statewatch News, 2003; Reporters without borders, 2004).

In 2003, the Home Office initiated a second public consultation in form of two consultation papers, one on access to communications data (Home Office, 2003a) and one on the retention of communications data (Home Office, 2003b). These

provided some background and further justifications for the need for a range of public authorities to access communications data as a necessary and proportionate requirement. For example, the consultation paper 'Access to Communications Data - Respecting Privacy and Protecting the Public from Crime' (Home Office, 2003a) seeks consultation regarding permitting access to only *parts* of communications data, that is service use information and subscriber data, to *certain* public authorities.

After this consultation period, Parliament approved the implementation of Chapter II. In summer 2006 the Home Office published a further consultation paper relating to Chapter II, Part I of the RIP Act to invite comments regarding the revised draft code of practice (Home Office, 2006). In September 2003, the Home Secretary proposed a new amendment to the RIP Act. As before, this amendment gave many bodies including local authorities, the power to access communications data of citizens. The government appointed an Interception of Communications Commissioner to protect citizens from abuses of the RIP Act and ATCS Act (Reporters without borders, 2004). Sir Swinton Thomas was appointed as the Interception of Communications Commissioner from 11 April 2003 to 10 April 2006 under Section 57(1) of the Regulation of Investigatory Powers Act 2000. His role requires him to publish annual reports which review the interception processes (see for example Swinton, 2007). Hosein argues that instead of making the retention of communications data mandatory in UK, the government took the issue to Europe (Grossman, 2006).

The following table (Table 2.2) gives details about reasons for access and organisations that are entitled to gain access to communications data under the RIP Act:

Table 2.3: Access to communications data: reasons and organisations

Communications data can be obtained for the following reasons:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
- for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(Home Office, 2000, Chapter II, section 22)

The following organisations hold the powers to obtain communications data:

- Any Police Force including PSNI, any Police Force of HM Forces and British Transport Police
- National Criminal Intelligence Service (NCIS)
- National Crime Squad (NCS)
- HM Customs & Excise
- The Inland Revenue
- The Security Service (MI5)
- The Secret Intelligence Service (MI6)
- The Government Communications Headquarters (GCHQ)
- Local Authorities such as FSA, DTI, the Emergency Services; government departments such as DEFRA, Dept of Health, Home Office Immigration Service; as well as County and District Councils (see SI 2003 No 3172).
- Department of Work and Pensions

(The Investigatory Powers Tribunal, 2005)

Communications data can be obtained by the authorisation of a relevant and named senior official of an organisation listed in Table 2.2, who must consider the request for communications data to be necessary and proportionate in order to authorise it. There is a much wider range of purposes, such as public safety, preventing serious harm or collection of tax (see Table 2.2, above), than those for which a warranted interception of a communication can be made in order to obtain the content of the communication (Davis, 2003). As explained in the previous section 2.3.2, the content of communication is considered as more intrusive than information about the communication.

There is a requirement for organisations to liaise with Communications Service Providers through a Single Point of Contact (SPoC) to ensure the smooth provision of service by CSPs. A SPoC is "an individual or group of individuals within a public authority who has been trained and accredited to facilitate lawful access to communications data" (Home Office, 2003a, section 9). SPoCs assess whether access in a particular case is reasonably practical for the CSP and also consider costs and resource implications for the CSP and the public authority. The Interception of Communications Commissioner oversees authorisations of access to communications data. CSPs may be compensated for the costs involved in retaining and giving access to data, with money that may be provided by Parliament (RIP Act, section 24). The Office of Surveillance Commissioners (2003) provides an oversight of the conduct of covert surveillance by public authorities according to Parts II and III of the RIP Act.

2.3.3.2 Anti-Terrorism Crime and Security Act 2001 (ATCS Act)

The Regulation of Investigatory Powers Act 2000 did not require communications service providers to retain data, and instead only regulated access to the data that may reside in CSPs networks. However some mobile phone service providers had admitted to store communications data for months and years (Millar and Kelso, 2001), which would not have been permitted by the Data Protection Act 1998 (section 2.2.3.2). The Anti-Terrorism Crime and Security Act 2001 provided a legal basis for the retention of data and specified periods of time during which communications providers would be required to retain communications data.

In August 2000, a proposal to store communications traffic data for up to 7 years was submitted to the Home Office by the National Criminal Intelligence Service (NCIS) on behalf of a number of UK law enforcement agencies, such as MI5, MI6, the Association of Chief Police Officers, and GCHQ (Ahmed, 2000). The reasons

given for these proposed changes were the growing need to fight cyber crime, international drug trafficking and the use of computers by paedophiles (Privacy International, 2002; Whitley and Hosein, 2005). The author of this report was the Deputy Director-general of the NCIS, which oversees criminal intelligence in the UK. The document proposed giving access to the retained communications data under the provisions of the RIP Act. Communications data was suggested to be retained for real-time access by communications service providers for 12 months. Once the data was 12 months old, it should be retained for a further six year period and deleted afterwards. Mobile phone location data was described as beneficial to investigations, as it could be used to locate the proximity of a mobile phone user to a crime scene, to trace associates of suspects and to locate places of significance. Oversight was proposed to be given by the designated chief officer (Gaspar, 2000).

This proposal was never formally adopted as government policy, even though the government's policy did change in the months and years after. In addition, capturing traffic data of all citizens was not seen, at the time, as a reasonable and proportionate response to the growing use of new technologies by criminals. Britain's Deputy Data Protection Commissioner pointed out that the retention of traffic data would constitute a conflict with the right to privacy as laid down by Article 8 of the Convention on Human Rights (Ward, 2001).

This situation changed with the introduction of ACTSA. The Anti-Terrorism Crime and Security Bill was introduced to Parliament two months after the September 11, 2001 attacks and received the Royal Assent already on December 14, 2001. The bill passed through the House of Commons with the government allowing it only 16 hours of debate, which was seen as an inappropriate length of time, considering the complexity of the Bill and the extensive number of 129 sections. While the House of Commons did not impose a single amendment on the Government, the House of Lords voiced more opposition to the Bill. A number of Lords who are also lawyers warned that the Human Rights Act could not provide a sufficient safeguard against the illiberal measures (Fenwick, 2002). The swift schedule of introducing and debating the Act has led a Parliamentary Committee to question whether the Act had been discussed and examined in sufficient detail, as its provisions result in major implications for civil liberties (Select Committee on Home Affairs, 2001). Others consider that the September 11 attacks served as a blanket reason for establishing measures that had been previously in preparation by government departments (Whitley and Hosein, 2005).

Tomkins (2002) criticises the Act as “the surely the most draconian legislation Parliament has passed in peacetime in over a century”. Other commentators refer to the Home Secretary's “mantra that they are merely protecting democracy” (Fenwick, 2002, p. 724), and warn that “draconian anti-terrorist laws have a far greater impact on human rights then they ever will on crime” (Wadham, 1999).
Indeed, supporting this view is the fact that a voluntary code had been agreed between government and the communications industry (section 102.4). The ATCS Act requires communications service providers to voluntarily retain communications data "to safeguard national security or to prevent, detect or prosecute crimes related to national security" (ATCS Act, 2001, explanatory notes, Section 29). These voluntary requirements can be made mandatory if deemed necessary by the Secretary of State (ATCS Act, 2001, Section 104). Walker and Akdeniz (2003, p. 14) point out that this might indicate “how hesitant Parliament felt about the grant of these powers”.

At first a draft Code of Practice was established, which was consulted upon (section 103.1.a and b) and then brought before Parliament (section 103.4). The Act allowed the Secretary of State to make the Code of Practice compulsory (section 104). Whitley and Hosein (2005) point out that the Code did not introduce the process of data retention in the UK. A sunset clause was included within ATCS Act, which meant that if the government failed to introduce a Code of Practice within two years, the provision would not be implemented (Reed and Angel, 2007). The ATCS Act builds on the anti-terrorism measures enacted in the Terrorism Act 2000, such as the extension of police powers, and the implementation of criminal co-operation measures under the Third Pillar of the EU (Shah, 2005). The September 11 attacks have let to the introduction of additional powers addressed specifically to international terrorism, however many of these powers contained in the ATCS Act were to prove even more contentious than the provisions of the Terrorism Act 2000 which they complement (Bradley and Ewing, 2007).

The ATCS Act sets the maximum retention period for data held under the provisions to 12 months, whereby longer retention periods may be justified by the business practices of the communication service provider (Home Office, 2003c, section 16). The Act contains regulations dealing with terrorism and protecting national security, such as terrorist finances (part 1-3), racial hatred (part 5), bribery and corruption (part 12). Part 4 made it possible for the Home Secretary to detain non-British terrorist suspects indefinitely, which was deemed to be incompatible with the

European Convention on Human Rights and ceased to be in force. Relevant for data retention is Part 11, as it deals with the retention of communications data for national security purposes. The retention of communications data is a form of personal data processing, and hence it is subject to the Data Protection Act 1998. Oversight of the 1998 Act is by the Information Commissioner (Home Office, 2003c, Section 29).

The provisions made in Part 11 amend the RIP Act so that communications service providers must retain communications data and disclose it to secret intelligence and law enforcement agencies far more extensively than the RIP Act had initially envisaged. The Parliamentary committee for human rights, that is the Joint Committee on Human Rights expressed concern about the rule-making authority of the Secretary of State by this part of the Act (HL 51, HC 420, 2001-02). For example, the Secretary of State may add to the organisations that can obtain communications data and increase the purposes for which the data can be obtained. This is perceived as controversial since this enables the Secretary of State to greatly increase the ability of public authorities to acquire information about citizens and organisations (Davis, 2003). Finally, the Secretary of State had been made required to publish the code of practice in draft, consult with the Information Commissioner and not to bring the code into effect until it had been approved by both Houses of Parliament. The Information Commissioner also showed concern and referred to earlier discussions about communications data retention:

> "**The Commissioner has been aware for some time of pressure from the law enforcement community to require communications providers to retain details of communications data.** This, it is claimed, would assist the detection of particular crimes and help with criminal intelligence gathering. Although such calls have been made it has not always been clear to what extent such retention is required beyond the period for which the communications providers would retain this for their own business reasons"
>
> (HL 51 and HC 420, 2001-02)

The ATCS Act was perceived as controversial for mainly two reasons. Firstly, some of the anti-terrorist powers are seen to be disproportionate to the actual threat facing the UK. It does for example not seem adequate to include Part 11, which deals with the retention of communications data, in an emergency Bill that had to be rushed through Parliament (Shah, 2005). Secondly, it has been argued that there is a lack of connection to the September 11 attacks, as the Act contains miscellaneous provisions that relate to criminal law and criminal justice matters, as well as it

increases the general powers of the police and other governmental agencies. One example of these new powers is ACTSA Part 11, which is about the new Code of Practice on retention of communications data (Fenwick, 2002; Davis, 2003). The Act also included an extension of already controversial police powers, as it amended the Police and Criminal Evidence Act 1984 and the Criminal Justice and public order Act 1994 (Shah, 2005).
Lord Waddington, a former Home Secretary, also argued that some of the legislative measures where not related to the September 11 attacks, as for example

> "The proposal to make incitement to religious hatred a criminal offence has been hanging around in the Home Office for a long time, at least since 1985 when it featured in a Law Commission report. So it has precious little to do with the events of September 11th (..)".
>
> (HL Debate, 2001)

In its jurisprudence, the European Court of Human Rights found that retention of data by governments constitutes an interference with a citizen's right to respect for private life (Article 8.1), whether or not the governments use the data against the individual. For example in the legal case of Rotaru v Romania (2000, App. no. 28341/95), the ECtHR found a violation with Article 8 took place, when the Romanian security services had stored information on Mr Rotaru's past activities as a university student. Privacy International (2003a) has argued that the data retention as put in place by ATCS Act is more invasive than this case, even though it is only the traffic data that is stored and not the content.

Davis (2003) claims that proportionality as a human rights concept has the most considerable impact on the law of the United Kingdom. The doctrine of proportionality provides that any interference with a Convention right must be "proportionate to the legitimate aim pursued by that interference" (Whitty, Murphy, Livingstone, 2001). Three criteria need to be met to satisfy the proportionality test; firstly an immediate and very serious threat should be evident, secondly measures that are designed to meet the legislative objective must be connected to it, and thirdly the measures should not go further than needed to combat the threat. Fenwick (2002) argues that the "ATCS Act fails to meet the first and last of these tests", and as discussed above, some claim that some of ATCS Act's provisions are not connected to the September 11 attacks.

2.3.4 European Data Retention Directive (2006/24/EC)

The importance of the role that communications data can play in crime and terrorism investigations had been recognised by European enforcement agencies. However, the long-term retention of every citizen's communications data had been treated with hesitation before the September 11 attacks in the US. In response to the attacks, the cooperation on criminal affairs of a wide range of European law enforcement agencies on fighting terrorism had increased while previously the jurisdiction over police matters was mainly national and so were the rules for data protection (Bignami, 2007).

The Data Retention Directive 2006/24/EC of the European Parliament and of the Council was approved on 15th March 2006 after lengthy negotiations. The Directive was seen to affect the balance of power between the privacy of individuals and the right of the state to protect national security. It gives rise to a significant change in the basic principles of personal data protection (Davies and Trigg, 2006). According to Stefano Rodota (2006), then-chairman of the EU's Article 29 Data Protection Working Party highlights, any changes affecting data protection have an effect on the degree of democracy of European citizens, since the protection of personal data is an important element of freedom in society. The dynamics in the run up the final approval of the contested Data Retention Directive were complex and numerous stakeholders (such as the European Union institutions, civil liberties groups) were involved in the negotiations.

The European Data Protection Commissioners had been aware of the law enforcement agencies' desire to for the long-term retention of communications data (Statewatch News, 2001b). Before the 11 September attacks in the US, the tone in the European Parliament had been largely critical of data retention proposals. The long-term retention of communications data had been largely dismissed as "improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the ECHR", as for example by the Data Protection Commissioners in the EU at their spring conference in April 2000 (Munir, 2005). In July 2001 the European Parliament's Civil Liberties Committee approved the draft Directive on Privacy and Electronic Communications without data retention. A report by the radical MEP Marco Cappato argued that EU should restrict the powers of law enforcement agencies regarding the retention and access of communications data, and also rejected proposals to retain traffic data for up to seven years (McAuliffe, 2001).

However, shortly after the September 11 terrorist attacks, in October 2001, external pressures from the US were applied to European Union representatives. President George W. Bush sent a letter to the European Commission President Romano Prodi, which made a suggestion to retain data that would otherwise be destroyed under the European Data Protection Directives to counter terrorism: “Revise draft privacy Directives that call for mandatory destruction to permit the retention of critical data for a reasonable period” (Statewatch News, 2001). Despite these propositions to the European Union, the US does not require communications service providers to retain communications data of all of its customers but instead uses data preservation, which means that only data about certain suspect users is held. Nevertheless, in the US communications service providers may store traffic data for marketing purposes, whereas in Europe, the CSPs used to be required to erase this type of data as soon as it is no longer needed for billing purposes (Bignami, 2007).

Until a few weeks before the final vote on 30th May 2002, the majority of the Members of Parliament opposed any form of data retention. However, after pressure by the European Council and European Union governments, parliamentarians voted in favour of the Council's position on data retention (EPIC, 2007). The EU Directive 2002/58/EC on Privacy and Electronic communications was adopted on 25 June 2002, and states that member states may now pass laws permitting the retention of internet and mobile phone communications data. It leaves each EU member State free to adopt laws authorising data retention and it could be argued that the Directive encourages the retention of data, which can be seen as the first step towards the development of a more detailed data retention Directive. The Directive 2002/58/EC reverses the position of the 1997 Telecommunications Privacy Directive by explicitly allowing EU countries to require communications service providers to store the communications data of their customers:

> “Member States may adopt legislative measures […] when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system […] Member States may, inter alia, adopt legislative measures providing **for the retention of data** for a limited period justified on the grounds laid down in this paragraph.”
>
> (Directive 2002/58/EC, Article 15)

The 2002 Directive in its Article 6 requires CSPs to *erase* all traffic data that is no longer needed for providing services. This however had been changed in the 2006 Data Retention Directive, which allowed exceptions in its Article 15.1.

A 'Questionnaire on traffic data retention' was distributed by the Danish presidency of the EU to all Member State's governments in August 2002. The objective was to collate comments regarding the practice and experiences of traffic data retention in European member states in order to "facilitate the development of strategies and working agendas" (Questionnaire on traffic data retention, 2002). The responses showed that 10 out of 15 member states already had a legal obligation to store traffic data or were finalising a new legislation (Responses to the data retention questionnaire, 2002). A new questionnaire was issued two years later to obtain the practices of the new European member states (Questionnaire on traffic data retention 10767/04, 2004).

After the train bombings on March 11 2004 in Madrid, in which telecommunications played an important part, a proposal for the European-wide retention of communications data was debated at the EU spring summit end of March 2004 (Blakeney, 2007). Following this, in April 2004, the UK together with France, Ireland and Sweden submitted a joint proposal to the European Union for a framework decision on the retention of communications data for between one and three years or possibly longer. Interestingly, Spain, the country where the bombings had taken place, was not involved in this proposal. This data retention proposal suggested retaining communications data to "increase prevention, investigation, detection and prosecution of criminal offences, including terrorist acts" (Alvaro, 2005; Statewatch News, 2005a). This proposal was widely criticised. The Article 29 Data Protection Working Party in its opinion from November 2004 reiterated its previous view that the mandatory retention of communications data was not compatible with human rights and privacy laws and in conflict with the current data protection legislation. In addition, they raised concerns about the cost of the European-wide implementation (Article 29 Data Protection Working Party, 2004).

Finally, in June 2005, the controversial data retention proposal was partly deemed illegal by the Legal Services of both the European Council and Commission (Statewatch News, 2005b; EDRI, 2005a). This legal opinion was based on the fact that the proposed legislation about data retention was put forward as a framework decision. A framework decision is a legal instrument under the third pillar (criminal

law, policing), where the European Parliament only has a consultation right but no real influence. However, the proposed legislation should have been presented under the first pillar (economic, social and environmental policies) as it contained obligations addressed to civil parties, namely the service providers to retain and collect data. However, placing the legislation under the first pillar would have weakened the proposal because Directives cannot create substantive and enforceable rights. A Directive has distinct objectives but leaves the national authorities the choice of form and method within a set time frame (Storey and Turner, 2005; informal talk with a desk officer for this dossier of the European Union).

The Article 29 Working Party criticised the Data Retention Directive again in their opinion issued in October 2005. They argued that “Traffic data retention interferes with the inviolable, fundamental right to confidential communications” and that this should be limited to exceptional cases (Article 29 Data Protection Working Party, 2005). As mentioned above, the Working Party had continuously questioned the appropriateness of the mandatory data retention regime and issued 20 recommendations which, however, were not fully taken into account (Davies and Trigg, 2006).

The Data Retention Directive 2006/24/EC amended the Directive 2002/58/EC on Privacy and Electronic Communications, by adding a paragraph allowing data to be retained for purposes stated in the 2006 Directive, which are "investigation, detection and prosecution of serious crime, as defined by each Member State in its national law" (Directive 2006/24/EC, Article 11). The Data Retention Directive aims to harmonise obligations on communications service providers of the EU member states but does not aim to regulate the technologies for retaining data. Communications data shall be retained for a period between six months and two years (Article 6). Exceptions are possible, so that data can be retained for longer periods (Article 12). The Directive requires member states to introduce laws complying with this Directive by 15 September 2007, however all members states asked to postpone parts of the application of the Directive until 15 March 2009 (Article 15). For example, the UK has asked to postpone the retention of internet access, internet telephony and internet email.

There is the possibility for criminal law sanctions for intentional access or transfer of data that is not permissible under national law (Article 13). Access to data shall be

provided to the competent national authorities (Article 4). However as Davies and Trigg (2006) points out, a harmonisation of approaches between member states might be difficult, considering the lack of equivalent law enforcement authorities. Each member state should appoint a public authority to be responsible for monitoring the security of the stored data. This should be the same authorities as those referred to in Directive 95/46/EC (Article 28), which is in the UK Office of the Information Commissioner, an independent government authority and reports directly to Parliament. The Directives leave the issue of who is going to pay for the retention of communications data up to the individual member states. Critics of the 2006 Data Retention Directive point out that the Directive does not provide a clear definition of offences, nor procedures for data access. It does not specify security measures required to safeguard the data, which may result in an increased risk of breach of privacy in member states with weaker data protections. Finally, the Data Retention Directive 2006/24/EC does not provide a definition of "serious crime" and this may hence lead to different definition in the member states, the same is true for penalties that may be imposed upon failure to comply with the regulations resulting from the Directive (Data Protection Working Party, 2004; Vilasau, 2007).

2.3.5 Discussion about the rightfulness of communications data retention

All groups involved in the discussion acknowledge that the retention of some communications data is a useful tool for tackling cyber crime and terrorism, as it serves as evidence of mobile phone and internet communications. However, there are various arguments against the retention of communications data of *all* citizens for 12 months in the UK (up to 24 months under the European legislation) and access to this data by a range of governmental agencies in the UK.

2.3.5.1 Argument 1: Objection on the ground of human rights and civil liberties

The violation of human rights is the most frequently used argument against the retention of all European citizens' communications data for an extended period of time (see also 2.3.3.2). The retention of communications data by service providers for longer periods than for business purposes can be seen as conflicting with the European Convention on Human Rights, specifically with Article 8 'Right to respect for private and family life'. In 1998 the Parliament approved the Human Rights Act to incorporate the European Convention on Human Rights into UK law, which established an enforceable right of privacy in British law for the first time in history.

Article 8.1 provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this is subject to restrictions and there can be interference by a public authority "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (ECHR, Article 8.2). As the data retention legislation is implemented to assure national security and support the fight against terrorism, European member states can implement the Data Retention Directive in accordance with Article 8 ECHR.

Since the Human Rights Act 1998, human rights standards have been routinely incorporated in legislation. Under section 19(1)a of the HRA, Ministers responsible for introducing government Bills to either house need to provide a written statement that in her or his view, the Bill is compatible with the Convention rights, or alternatively that it is not compatible and that the government nevertheless wishes the Parliament to enact the Bill into law. The Home Secretary made this compatibility statement with regard to the ATCS Act, however, the ATCS Act contains a number of provisions that affect human rights, which make the Act is not compatible with HRA. For example, the detention without trial is incompatible with the right to liberty of the person under ECHR Article 5(1), and this required a formal derogation from Article 5(1) under Article 15 of the ECHR (Tomkins, 2002, p. 7; HL38, HC 381 (2003-04).

Privacy International (2003a) argues that ‘‘blanket data retention would subject every citizen to the certainty of ongoing and unremitting interference in his or her private life’’. The richness of mobile phone communications data which conveys who has been contacted when and from where for how long, makes it possible to compile a detailed profile of a person's interests, including communications patterns, network of acquaintances and social context. Data relating to mobile communications is more sensitive than those associated with traditional fixed telephony, as it conveys the location at the beginning and end of call, as well as details about text messages exchanged with other parties. Converging platforms and infrastructures, such as internet and mobile phones increase the sensitivity of traffic data, for example when mobile phone handsets are used to access the internet (Escudero-Pascual and Hosein, 2004). Communication technologies, such as mobile phones and email, serve as everyday means of communication in private and business life in Britain and the rest of Europe. They are a vital element of

modern life and the blanket storage of all communication transactions does not give citizens a choice to circumvent this type of mass surveillance. It could be argued that individuals can be discriminated from taking part in essential interactions with friends, family, businesses and employers when trying to avoid the use of modern means of communications.

2.3.5.2 Argument 2: Data preservation instead of retention

The question whether the retention of all citizens' communications data is proportionate is also at the heart of data retention debates (see for example Whitley and Hosein, 2005). Data *preservation* instead of data *retention* is seen as a more proportionate measure in responding to terrorism than a blanket data retention regime requiring the storage of all citizens' data (European Data Protection Commissioners in Home Office, 2003b). Data preservation is more targeted than data retention, as CSPs are requested only to retain data on a case-by-case basis, which means data about a particular user for a specified period of time. For example, the Data Protection Working Party had in their Opinion 05/2004 suggested the use of less invasive mechanisms, such as the so-called “quick freeze-procedure”. Instead of a general storage of all data, this system would have allowed law enforcement authorities to request the service providers to store particular data and to obtain a court order to access this data (Article 29 Data Protection Working Party, 2005).

However, this approach has been rejected by the Home Office as data preservation "will never aid in the investigation of a person who is not currently suspected of involvement with a terrorist organisation" (Home Office, 2003b, p15).
It is also debated whether surveillance of communications data can help to prevent terrorist attacks at all. Tony Blair is quoted to have said that "all the surveillance in the world could not have prevented the London bombings" (Davies, 2005).
A Dutch study by the Erasmus University claims that data retention is unnecessary based on a review of 65 police investigations. 'In virtually all cases' the police could get access to all traffic data required based on existing account and billing information retained on average for three months (EDRI, 2005b).

2.3.5.3 Argument 3: No definite link between communications device and user

Communications data cannot be linked without any certainty to a personal identity, thus blanket data retention is ineffective in fighting crime. Even though communications data can serve as evidence for crimes planned with help of communications technologies, an undoubted link between the device that had been used for communication and an individual can not be established with any certainty and further investigations, according to Walker and Akdeniz (2003). This becomes particularly apparent when a web-based email system such as Hotmail is used from a PC in an internet café, as Microsoft's Hotmail does not verify details of registered users and internet cafés do not require identification. The use of prepaid phones that do not need registration poses a challenge to law enforcement agencies, as they do not require the subscriber to be identified (Gow, 2005).

2.3.5.4 Argument 4: High cost of storage and retrieval of data

The telecommunications and internet industry have highlighted the high costs for storage and searches of the retained data, as legislation requires CSPs to store communications data for longer than needed for billing purposes. The internet Service Providers' Association (Ispa) expects costs of £26 million a year to set up sufficient data retention measures and £9 million in running costs to respond to law enforcement requests based on estimates from one large UK-based internet service provider (Leyden, 2005).

The requirement of communications service providers to store the customers' data for up to two years and the costs associated with it could also affect global competitiveness of the European industry compared to other western countries. Particularly as countries such as US and Canada have rejected the blanket retention of communications data. At the same time some fear that data retention may have an effect on consumer confidence, as citizens may avoid using electronic commerce in order to not have their legal transactions logged (Open Letter from civil society groups, 2005).

2.3.5.5 Argument 5: Potential use of data for other purposes

With the introduction of the ATCS Act, communications service providers are now required to keep customer records which they previously had to erase or anonymise. Under the Data Protection Act 1998 data could not be kept for any longer than necessary (fifth principle) and the data stored had to be adequate and relevant for purposes and not excessive (third principle). The DPA 1998 implements the European Union Directive 95/46/EC and governs the collection and process of personal data of individuals by the government and private sector.
As the current data retention legislation obliges CSPs to keep various types of customer data for longer than before, there are concerns that the data may not only be stored for the access by police and other public authorities but also for commercial purposes, such for consumer profiling, marketing purposes and CRM (customer relationship management). Green (2006) points out that the requirements of the state for long-term retention of communications data coincide in an unprecedented way with the extensive data-gathering practices of the telecommunications industry.

The retained communications data is also of interest to the music and recording industry to investigate music piracy and illegal file sharing in the European Union. The Creative and Media Business Alliance (CMBA), which represents large companies in the entertainment industry such as Sony BMG, Disney and EMI, has suggested to members of the European Parliament to be included in the latest European Directive on data retention (Sherriff, 2005; Thompson, 2005).

An additional concern regarding the use of data for law enforcement is that the European Data Retention Directive (2006/24/EC) does not define the term 'serious crime' used in its Article 1. In the same manner, the RIP Act allows access to communications data under a wide range of purposes, such as public safety or protecting public health (see section 2.3.3.1). Tony Bunyan, editor for Statewatch points out that the retained communications data maybe also be of interest to future uses of governments, as the data could be used for social and political control (Statewatch News, 2005c).

2.3.6 Synopsis of data retention discussion

The retention of some communications data to be accessed by law enforcement agencies is seen as beneficial and is supported by all stakeholders involved. The central elements for debates have been whether the blanket retention of *all citizens*' data for an *extended period of time* is justified and proportionate for the purpose of fighting terrorism. In the UK, there are discussions about whether some agencies should only have access to *certain* types of communications data, as traffic data is seen as more sensitive than user and service data. As a result of the 2003 consultation process, access by numerous agencies to communications data has been deemed justified by the Home Secretary.

A strategy of data preservation is favoured by many parties, as it would not infringe on the privacy of innocent communications users. In addition, this would also save money to the CSPs as less data would have to be stored and accessed in response to requests by eligible organisations under the RIP Act. Nevertheless, preservation is not seen as sufficient by the Home Office, as this would only enable access to data for a limited time before it would be deleted by communications service providers. The main issue seems to be whether retention of data is seen as proportionate and the responses by stakeholders differ widely.

2.3.7 Summary Part 3

The third and last part of this chapter has introduced the legal framework as relevant to the retention of mobile phone communications data in the UK. It has become apparent that a complex interplay is taking place between the national legislation in the United Kingdom and the European legislation, such as the European Convention on Human Rights. This section has detailed the legal instruments relevant to communications data retention: the Regulation of Investigatory Powers Act 2000, the Anti-Terrorism Crime and Security Act 2001 and the European Directive 2006/EC/24. Legislation on data retention has been widely debated within the United Kingdom and the European Union, from its initial introduction to the implementations of the RIP Act and the ATCS Act in the UK and the Data Retention Directive 2006/24/EC by the European Union. The section has painted a picture of data retention in legislative terms, while carefully ensuring to consider the viewpoints of the most relevant stakeholders in the debate the retention.

2.4 Summary of chapter

The multidisciplinary nature of the subject area of mobile phone location data and the long-term retention of communications data retention in general have been addressed with a threefold approach. This chapter has firstly focused on recent technological developments regarding mobile phone location data within the UK, followed by a discussion of privacy in the literature. The last part has provided essential background to the legislative landscape of the UK and the European Union.

Mobile phone location data is an inherent part of mobile communications, and advances in computer technologies have facilitated the long-term storage and analysis of this data. Communications data may be obtained and used by law enforcement for crime and terrorism investigations but also by commercial providers to offer services based on location. The widespread use of information and communications technologies for administrative and control purposes is seen as a trait of surveillance societies. The potential of inappropriate use of the retained communications data may result in infringements of the mobile phone user's privacy, which makes checks and safeguards to ensure accountability necessary. Before the September 11 attacks there had been widespread criticism of the long-term retention of communications data. However, the attacks have been used in the UK and EU-wide to evoke a paradigm shift in storing and accessing this type of data. The retention of data was justified under Article 8.2 of the European Convention on Human Rights, but the wide range of purposes for which the data can be accessed under the Regulation of Investigatory Powers Act 2001 and the European Data Retention Directive 2006/24/EC, have been widely criticised.

The next chapter focuses on the methodology that has been used to collect empirical data in order to portray the views of ordinary citizens in the complex debate about technological influences on individual privacy.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 3 Research Methodology

This chapter introduces the research methodology used for this study and how it has guided data collection, analysis and development of theory. Firstly, essential background and fundamental guidelines common in different approaches to grounded theory methodology (GTM) are provided. The subsequent three sections describe the data collection phases for this study, which consisted of a mobile phone tracking pilot study, in-depth interviews and a survey. The chapter concludes by explicating the analysis approach for the empirical data.

3.1 Grounded theory methodology - an overview

"If someone wanted to know whether one drug is more effective than another, then a double blind clinical trial would be more appropriate than grounded theory study. However, if someone wanted to know what it was like to be a participant in a drug study [..], then he or she might sensibly engage in a grounded theory project or some other type of qualitative study."

(Strauss and Corbin, 1998, p. 40).

Strauss and Corbin's quote above encapsulates the essence of when it is best to use grounded theory methodology for a research project. GTM provides useful tools to learn about individuals' perceptions and feelings regarding a particular subject area. Quantitative data may be useful in measuring attitudes across a large sample, however, GTM offers a powerful methodological framework if the aim of the study is to learn about individuals' perceptions.

GTM shares the following characteristics with other qualitative methods, which correspond to those of this study:

- Focus on everyday life experiences
- Valuing participants' perspectives
- Enquiry as interactive process between researcher and respondents
- Primarily descriptive and relying on people's words

(Marshall and Rossman, 1999)

Grounded theory originated in the 1960s in the United States in the fields of health and nursing studies. Barney Glaser and Anselm Strauss' influential book from 1967 'The Discovery of Grounded Theory' articulates the authors' research strategies for studies of patients dying in hospitals. Their successful collaborative study was perceived as a response to the predominantly quantitative research paradigms at the time. Grounded theory methodology advocates *creating new theory* consisting of interrelated concepts rather than *testing existing theories*. A study guided by GTM does not seek representativeness to achieve statistical generalisability but instead aims to explain and sometimes predict phenomena based on empirical data. The data collection typically encompasses in-depth interviews but can also include other sources of data such as existing research literature and quantitative data. GTM provides guidelines for data collection and analysis consisting of coding, comparisons between data, memo writing and theoretical sampling.

3.1.1 Data collection and analysis in grounded theory

GTM uses a form of purposive sampling, known as *theoretical sampling*, where participants are selected according to criteria specified by the researcher and based on initial findings. Early analysis of data indicates issues that need exploration; hence the sampling process is guided by the on-going theory development. Data collection and analysis take place in alternating sequences (see Figure 3.1). This can also be described as an iterative cycle of induction and deduction, consisting of collection of data and constant comparison between results and new findings in order to guide further data collections (Strauss and Corbin, 1990; Miles and Huberman, 1994). For these reasons the development and identification of variables does not take place prior to data collection but instead as part of the data collection process. Consequently, the variables or concepts are initiated by the interviewee and further developed and conceptualised by the researcher. Data is collected until *theoretical saturation* is

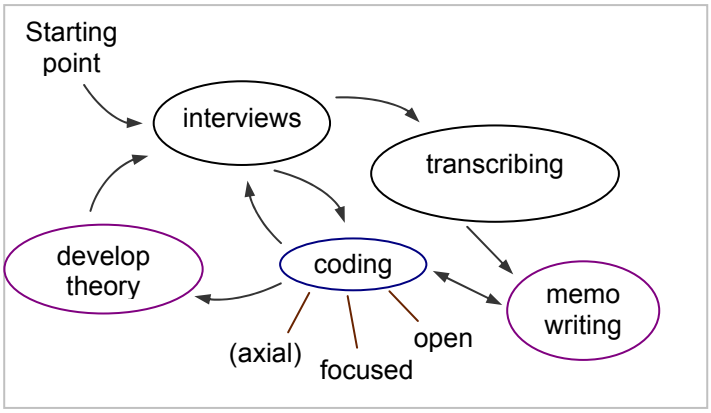


Figure 3.1: Steps in developing a grounded theory

reached, in other words until no new or relevant data emerges regarding a category and relationships between categories are established (Strauss and Corbin, 1998).

Interview questions should give as little guidance as possible to allow the interviewees to talk about what is of importance to them regarding a given context. The researcher then needs to extract those phenomena or experiences significant to the interviewee by assigning a conceptual label, known as a *code*. Several codes can be grouped into more abstract *categories* which will eventually form the basis for the developing theory.

3.1.1.1 Coding interviews as part of the analytic process

Interview coding is used to capture what is in the interview data, to learn how people make sense of their experiences and act on them. Coding is the first step of data analysis, as it helps to move away from particular statements to more abstract interpretations of the interview data (Charmaz, 2006).

Grounded theory methodology advocates using several coding techniques to examine interviewee's accounts at different levels. *Open coding*, also known as line-by-line coding, provides a good starting point to identify initial phenomena and produce a list of themes of importance to the interviewee. Conceptual labels are attached to almost every line in the interview transcript to capture what has been said. These labels can correspond closely to the interview context and when taken from the interviewee's own words, are known as *in vivo code*. Codes are assigned to participants' words and statements to develop concepts, constituting the start of the analytic process.

The detailed and meticulous process of line-by-line coding helps to open up the text and interpret the transcript in new and unfamiliar ways which also helps test the researcher's assumptions. Strauss and Corbin (1998) suggest using initial or 'sensitising questions', to help the researcher grasp what the data might be indicating. Suggested questions are "Who are the actors involved?", "What are the actors' definitions and meaning of these phenomena or situations?" (Strauss and Corbin, 1998, p. 77).

The next coding phase is more abstract than open coding and known as *focused coding* or selective coding. Focused codes are applied to several lines or paragraphs in a transcript and require the researcher to choose the most telling codes to represent the interviewee's voice. Using open codes as a starting point,

the process of focused coding helps to verify the adequacy of the initial concepts developed. As the focused codes will be applied and therefore 'tested' on further interview transcripts.

Another subsequent phase of coding is *axial coding*, defined by Strauss and Corbin as "the act of relating categories to subcategories along the lines of their properties and dimensions" (Strauss and Corbin, 1998, p. 123). The aim of axial coding is to add depth and structure to existing categories (see also 3.1.1.2, below). Charmaz (2006) explains that axial coding re-assembles data that has been broken up into separate codes by line-by-line coding. Strauss and Corbin (1998) use axial coding to investigate conditions of situations described in the interview, their actions and consequences. Charmaz (2006) warns that axial coding applies a too rigid and formal frame to the data analysis. Instead she recommends the less formalised approach of reflecting on categories, sub-categories and to establish connecting links between these to make sense of the interview data. The most abstract level of coding is *theoretical coding*, which explores the relationships that have been established between categories. Several ‘rules’ or “analytic coding families” are put forward by Glaser (1978) to develop an advanced analysis of the subject area.

3.1.1.2 Developing categories

The general process of how to code an interview and develop a theory is depicted in simplified form in Figure 3.2, below. After coding several interview transcripts a researcher can identify many issues that are of importance to the respondents. These issues are also known as *phenomena* and are assigned a conceptual label to become a *code*, also known as a *concept* by Strauss and Corbin (1998). Some codes or concepts will share the same or similar characteristics and can be pulled together into more abstract *categories*, which can typically be interlinked and build the basis for a theory.

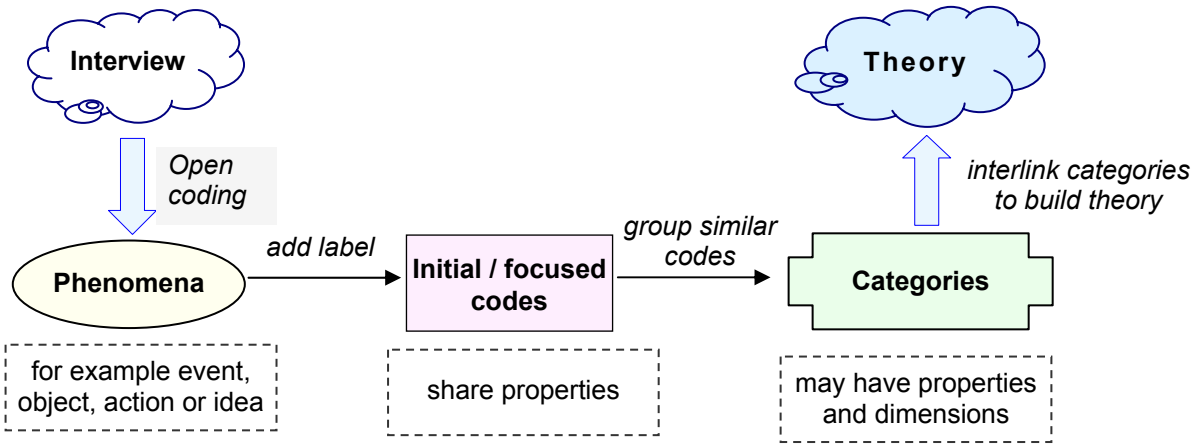


Figure 3.2: Coding steps in grounded theory (after Straus and Corbin, 1998)

It should be stressed that categories have to 'earn' their way into an emerging theory (Glaser, 1978). Grounded theory methodology typically does not use quantifying data to obtain meaning. However, counting the frequency with which categories occur in interview transcripts can be useful to confirm their importance for the interviewees. Categories can carry so-called *properties and dimensions*. A property is a general or specific characteristic of a category, whereas a dimension denotes the location of a property along a continuum or range (Strauss and Corbin, 1998). For example, the category 'phone ownership' could have the property 'spending' with dimensions ranging from 'low' to 'high spending'.

The central or *core category* is a distinctive category that sits at the heart of the developed theory and summarises what is happening. All other major categories should relate to the core category, which ought to appear frequently in the data (Strauss and Corbin, 1998). The development of the core category for this study is described in Chapter 4 - Presentation of Findings, section 4.2.4 to demonstrate the development of categories from codes.

Coding shapes the analytic frame and provides the skeleton for the analysis (Charmaz, 2006). Charmaz sees coding as an important link between collecting data and developing theory but also as a connection between empirical reality and the researcher's view of it. Coding highlights problems, issues, concerns and matters of importance to those being studied. Strauss and Corbin (1998) refer to categories as having 'analytic power', due to their potential to explain and predict. 'Constant comparisons' between collected data, codes, categories and initial findings help to crystallise ideas to become part of the emerging theory.

3.1.2 Use of grounded theory methodology for this study

The data collection and analysis for this study followed a cyclical process typical for GTM, by using early findings to shape the on-going data collection (see Figure 3.1). The pilot study involved tracking participants' mobile phones and conducting eight interviews. This data collection phase was followed by five more in-depth interviews that helped to explore issues raised in the pilot study. The survey aimed at exploring the research area on a wider scale than would have been possible with interviews being conducted and analysed by a sole researcher. More interviews were undertaken after the completion of the survey and these could address issues brought up by initial survey findings. Details about the sampling approaches for each of the three data collection phases can be found in the relevant sections in this chapter (3.2 Pilot study: Mobile phone location tracking , 3.3 Interviews, 3.4 Survey).

For this study, open coding was used for the pilot study interviews with the help of qualitative analysis software NVivo. However, using the software did not produce meaningful results and hence the pilot study interviews were re-coded with pen and paper after conducting the survey (see section 4.1.4 False starts with initial coding in NVivo). Focused coding was utilised for the next two interview phases, which used the initial codes as a basis. Axial coding was not used in this study because the method of specifying properties and dimensions for each category seemed too prescriptive and did not help the analysis of the data (see section 4.2.6 Importance of mobile phone settings). For the same reasons, theoretical coding was not adopted. Instead, careful comparisons between respondents' statements, as well as between codes and categories were undertaken, without being restricted to interpret participants' words within a framework of properties and dimensions.

The researcher's decision to use grounded theory methodology was only taken after conducting the pilot study. An initial analysis of the pilot interviews showed that it was not suitable to base the overall research project on existing theoretical models. The focus needed to be on participants' experiences and views of privacy and mobile phone location data. Hence an inductive approach was chosen to explore the subject area through the participants' eyes. The decision to use grounded theory methodology was further supported by the lack of existing theory regarding mobile phone location data and privacy.

Grounded theory scholars have different opinions about the most suitable time at which to review the literature. Glaser (1978) advocates waiting to conduct the literature review until initial findings have been made in order to not influence the researcher with preconceived ideas. This study has followed the advice of Charmaz (2006) and has carried out an initial review of the literature before the first data collection in form of the pilot study took place. The reason for an early review of literature was, on the one hand, to learn whether any similar research had already been conducted in this area and, on the other hand, to satisfy requirements of the university's research committee for the research proposal.

3.1.3 Substantive and formal theory

A grounded theory is directly related to the data from which it has been generated; it is therefore *grounded* in the data. Two types of theory are distinguished: substantive and formal theory.
Substantive theories provide a theoretical interpretation or explanation for a *particular* area, in other words this type of theory is used to explain and manage problems in a specific setting. Formal theories, however, are more abstract and provide a theoretical dealing of a *generic issue* which can be applied to a wider range of disciplinary concerns and problems (Strauss and Corbin, 1998). For example, a substantive theory can be about a limited area such as family relationships or professional education while a formal theory might deal with the construction of culture or the development of ideologies or stigma (Charmaz, 2006; Glaser, 1994). Charmaz (2006) suggests combining and conceptualising the results from several substantive grounded theories to develop a more general formal theory. Each substantive theory can help to refine the formal theory, in other words, a formal theory can relate to or 'cut across' several substantive ones. Charmaz (2006) points out that most grounded theories are substantive theories as they focus on particular problems in a specific, substantive area.

This study has developed a substantive theory as the collection of data and their interpretation focus on the explanation of a particular area, that is the relationship between mobile phone location data and individuals' perceptions of privacy in the UK. This PhD thesis does not provide the scope to raise the very specific, substantive theory to a formal theory that would be generalisable across a wider area, such as additional types of digital data or mobile phone users from other cultural backgrounds.

3.1.4 Memo writing

The process of coding and developing categories is supported by writing memos. Memos are a set of notes, that kept continuously, support the researcher by providing a record of thoughts and ideas. Memos enable the researcher to reflect on the interviews and given codes to enter into a dialogue about the collected data. Initial thoughts are of high relevance as they often spark the best ideas. Hence it is important to write the memo immediately when reading and coding the interview. At later stages in the research process, initial thoughts are represented through

memos and can be revisited, reflected upon and considered for the overall analysis. Memos can be used to ask questions, philosophise about potential meanings of interviewee's statements and compare concepts identified in interview transcripts to each other and to the literature.

3.1.5 Criteria for grounded theory studies

Charmaz (2006) gives the following criteria that grounded theory studies should aim for. She highlights that a combination of credibility and originality enhances the other two criteria resonance and usefulness.

a) Credibility
- Are there strong links between gathered data and argument?
- Are data sufficient to merit claims
- Do categories offer a wide range of empirical observations?
- Has the research provided enough evidence for the researcher's claims to allow the reader to form an independent assessment?

b) Originality
- Do the categories offer new insights?
- What is the social and theoretical significance of this work?
- How does grounded theory challenge, extend, refine current ideas, concepts and practices?

c) Resonance
- Do categories portray fullness of the studied experience?
- Does the GT make sense to the participants?
- Does analysis offer them deeper insights about their lives and worlds?

d) Usefulness
- Can the analysis spark further research in other substantive areas?
- How does the work contribute to knowledge
- Does the analysis offer interpretations that people can use in their everyday lives/worlds?

(Charmaz, 2006, p. 182)

Chapter 6, Conclusions and Recommendations, revisits these four criteria of grounded theory research and addresses how each criterion has been met by this study (section 6.4).

3.1.6 Objectivist and constructivist approaches to GTM

Grounded theory methodology has evolved since its inception in the 1960s in the United States. Particularly, the writings of Glaser (such as 1967, 1978), Strauss and Corbin (such as 1990, 1998) and Charmaz (e.g. 2000, 2006) are seen as influential for the development of GTM. The original work of Glaser and Strauss from 1967, 'The *Discovery* of Grounded Theory', suggests that the researcher should start collecting data with a 'blank mind', meaning without reviewing the existing literature in order to carry out a truly inductive study. Consequently, theory is built from observation and based on the understanding that the theory is already contained in the data and only needs to be dug up or *'discovered'*, as Glaser and Strauss' book title (1967) suggests. This perspective assumes that every individual will see and understand the data from the same point of view, making the same observations and therefore will come to similar conclusions. The researcher should take a passive stance and 'let the data emerge', which can be seen as a characteristic of an objectivist or positivist paradigm (Bryant, 2003; Charmaz, 2000). The alternative view in social sciences is the so-called constructivist or interpretivist view. Constructivist grounded theory methodology is for example advocated by Kathy Charmaz in her book 'Constructing Grounded Theory' (Charmaz, 2006). This strand of grounded theory methodology emphasises the research participants' experience and how *they* construct their view of reality. Knowledge, and hence the grounded theory, are constructed by both researcher and research participant and aim at interpreting the empirical evidence within the research context.

A divergence between the two authors of 'The Discovery of Grounded Theory' occurred in the 1980s, after which Glaser postulated his understanding of grounded theory methodology (Glaser, 1992). The late Strauss, however, together with his co-author Juliet Corbin, developed a different perspective on grounded theory methodology (Corbin and Strauss, 1990; Strauss and Corbin, 1998). The major difference between Glaser's and Strauss' views is Glaser's stance that "data emerges" and thus presents the same picture of facts to every researcher in form of some objective truth. Strauss' viewpoint on the other hand stresses that a researcher has to *actively* obtain theory from data. Hence, it is likely and even expected that each researcher will place the focus on different aspects of the collected data depending on their background, beliefs and values. Stern (in Morse ed., 1994) calls the former the Glaserian School and the latter Straussian School, as

both approaches to GTM differ in process and product and in her view represent completely different methods.

Charmaz (2000) argues that both Glaser's and Strauss and Corbin's approaches to GTM assume an objective external reality and hence take a positivist and objectivist stance. She, on the contrary, advocates a constructivist approach to GTM that assumes multiple social realities. Charmaz does not support the view that theories are discovered but believes that the studied world needs to be portrayed in an interpretive way because interviewee and researcher embark together on the process of constructing reality (Charmaz, 2006).
This study has been inspired and guided by Strauss and Corbin's and Charmaz' interpretation of grounded theory. The researcher disagrees with Glaser's stance that reality is objective and neutral, particularly regarding the intangible and personal subject area of privacy.

3.1.7 Limitations of the grounded theory methodology

Grounded theory methodology has limitations like any other research methodology. Some point out that GTM is very complex and time-consuming due to the tedious coding process and memo writing as part of the analysis (Bartlett and Payne in McKenzie et al., 1997). This study has dealt with the lengthy process of coding by using specialised software to help speed up organisation and analysis of data. Others name as a limitation that the use of GTM to explain, predict a phenomenon or to build a theory is a very subjective process, which relies heavily on a researcher's abilities. This study has followed the methodological guidance of Charmaz (2006) and Strauss and Corbin (1998) to gather and analyse the interview data. In addition, findings from the survey and pilot study were used to strengthen those findings based on interview data with the aim of fulfilling the criteria for GTM as described in sections 3.1.2 and 3.1.5. Many studies make use of the term grounded theory inappropriately and Bryant (2002) points out that the flexibility of the method can be used to provide a justification for studies lacking in methodological strength. Stern (in Morse ed., 1994) criticises some researchers for mixing methods such as ethnography and phenomenology and then use the label grounded theory to explain the analysis of their research findings.

The following three sections describe the data collection process for this study. Details about the findings and their analysis will be provided in the following two chapters, Chapter 4 and Chapter 5.

3.2 Pilot study: Mobile phone location tracking

The pilot study explored technical aspects of mobile phone location data and participants' perceptions of privacy regarding this subject area. Four participants' mobile phones were registered with an internet-based service provider that offered identification of the phones' geographical location 24 hours a day.
The aims of the pilot study were twofold: firstly to explore the technical side of location tracking by locating the participants with help of the commercial tracking service provider. Secondly, to learn about the participants' awareness of and attitudes towards location tracking in relation to privacy. Potential disadvantages of pilot studies were accepted and considered. These consisted primarily of the small sample size which could not provide representative results and the danger of making inaccurate predictions or assumption based on the pilot data.

3.2.1 Sample and ethical considerations

The participants were selected based on the researcher's judgement. This was due to the potentially invasive nature of the research design and the explorative characteristics of the pilot study. Two male and two female participants were chosen for the study and it was ensured that all four UK GSM mobile phone networks (O2, Orange, Vodafone and T-Mobile) were represented. It was a requirement of this study that all phones were operating on the GSM network in order to be locatable by any of the commercial mobile phone tracking providers. Out of the several internet-based companies offering similar mobile phone tracking services, one company was chosen for reasons of convenience and pricing. This service provider offered the registration of five mobile phones for £5 plus VAT per month. The phones of four participants and the researcher's phone were registered. Due to the small sample size and the limited age range of the participants (25 to 35 years), the study cannot be seen as representative for the overall population. The time span of four weeks was seen as a sufficient to generate a number of tracking results and to enable the participants to experience location data in their daily routines.

This study was guided by the ethical principles on research with human participants set out by Leeds Metropolitan University (Leeds Metropolitan University, 2006). Particularly the researcher's ability to determine a participants' geographical location 24 hours per day over a period of four weeks was perceived as the most profound ethical implication. The only possibility for a participant to not have his or her mobile

phone's geographical location identified would have been to either switch the phone off or to terminate the participation in the research project. For these reasons, the participants were informed about the study in great detail before asking for their consent to take part. Aims and objectives of the pilot project, together with details about the data collection process were explained to the participants. The participants were informed that they could withdraw from the study at any time without questions being asked. All data collected was anonymised by replacing the participants' names with ascending code numbers (P116 - P119) in the order of the initial interviews. Appendix A provides the email that has been sent out to the participants before giving their definitive agreement to take part in the pilot study.

3.2.2 Data collection procedures

After all four participants agreed to take part in the study, their mobile phone numbers were registered with the tracking service. The overall data collection had two main aims. For one part, to compare the geographical data that was generated by the location tracks to the participants' actual location. The second part aimed at exploring participants' perceptions, feelings and opinions regarding privacy, mobile technologies and particularly location data before and after the study. The data collection process is shown in Figure 3.3, below. 'Open track' denotes a location request known to the participant at the time of tracking and 'covert track' indicates a location request without the participant's knowledge.

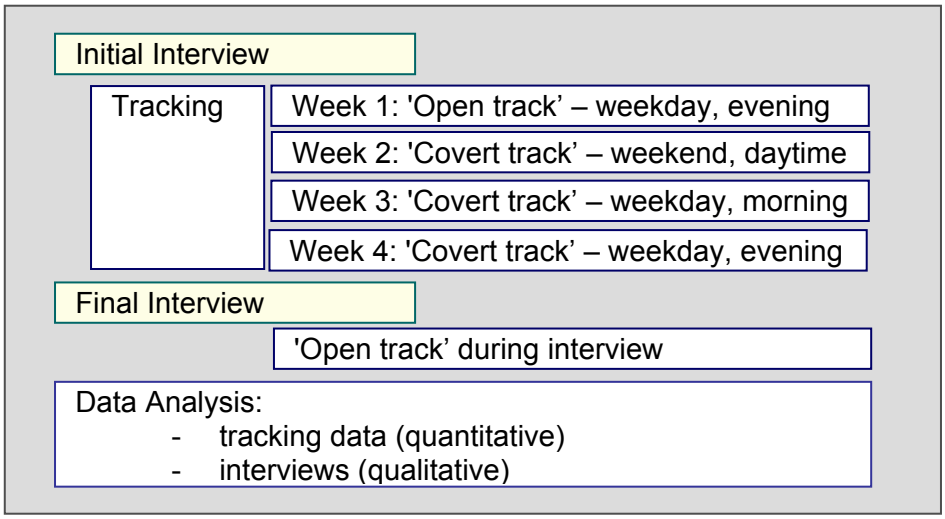


Figure 3.3: Data collection process for pilot study

3.2.2.1 Part one of pilot study: Location tracking of participants' mobile phones

A weekly location request was submitted for each participant over a period of four weeks and the results were stored electronically by the researcher. The participants were not contacted during this time to avoid influencing their tracking experience. The research participants could not know when a request for their mobile phone's geographical location was submitted to the tracking service provider.

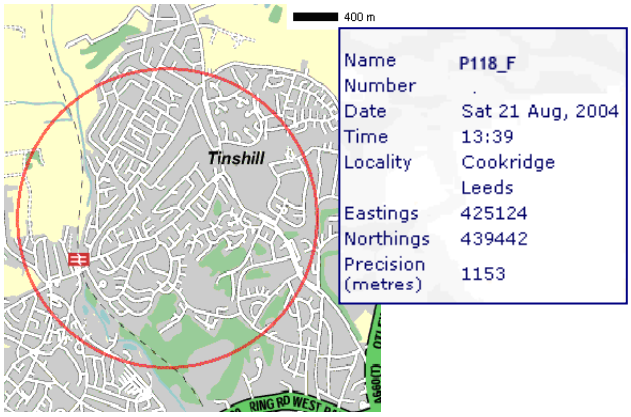


Figure 3.4: Example of location track

Figure 3.4 shows an example of a location request in form of a map depicting the participants' geographical location at the time of tracking. In order to be able to compare the participants' location provided by the service with their actual location, it was suggested to the participants to keep a location diary. To make it easier for the participants to recall their location at the time of tracking, the phones' locations were requested at different weekdays and times (see Figure 3.3). Immediately before the first location request only, all participants were contacted on their mobile phone. This phone call helped to familiarise them with the study and to obtain a first valid actual location. The participants were unaware of the three subsequent tracking requests. Hence, the participants' actual location had to be compared to the one supplied by the tracking service based on diary entries and memory in the final interview. A fifth track was conducted in the researcher's office as part of the final interview to demonstrate the service to the participants and to be able to compare the accuracy of tracking results between the four different mobile phone service providers.

Mobile phone tracking served two purposes, which tied in with the overall aims of this study. Firstly, mobile phone location tracking allowed comparison of the participants' location derived from location data with their actual whereabouts at time of tracking. The main purpose for this was to evaluate the service regarding reliability, validity and accuracy. Results from the location requests aimed at bringing location data into context with claims of privacy invasion through retention of location data. The researcher believes that police and emergency services have access to more detailed geographical data than a commercial tracking service provider. This assumption is based on media reports. However, using a commercial

service provider was seen as the only feasible way to get access to location data and to visualise this hidden aspect of mobile communication. The second purpose of location tracking was to raise the phone users' awareness of this type of data. The 'visualisation' of mobile phone location data by using a tracking provider proved to be a useful tool to enrich the qualitative data collection both for the participants and the researcher.

3.2.2.2 Part two of pilot study: Interviews

Respondents' perceptions and beliefs are at the heart of qualitative research and this was the main motivation for complementing the location requests with interviews. Semi-structured interviews were conducted with all four participants shortly before and after the four week tracking period to learn about their opinions and perceptions regarding mobile phone location data and privacy. The interview questions were of exploratory nature due to the small scale of this study and early stage in the overall research project. The questions were designed to identify patterns and common themes in the participants' accounts and sought to identify the meaning of privacy in relation to mobile phone location data in the participants' everyday lives.

During the interviews it was important not to restrain the participants but to give them time to talk about how they understood and described their experience of mobile phone tracking. This was particularly important as privacy is such an elusive concept, that can be perceived differently by different people. Figure 3.5, below, gives an overview of the interview themes and Appendix C - Interview questions for pilot study, provides a detailed list of interview questions.

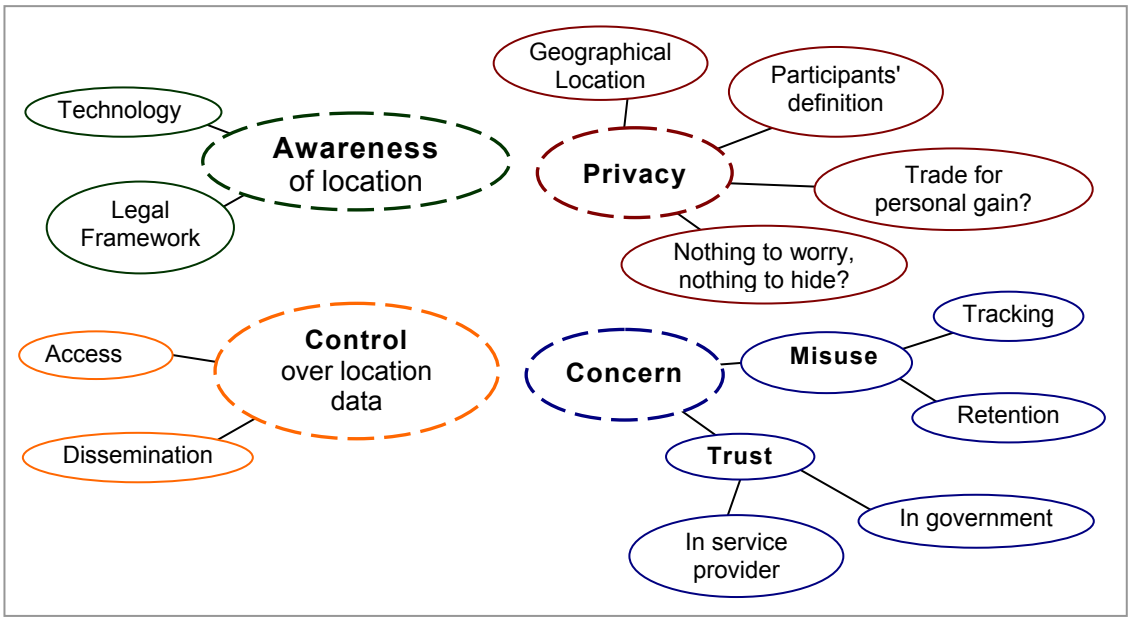


Figure 3.5: Graphical representation of interview themes

The interviews that took place prior to the tracking period focused on participants' awareness and knowledge of location data, as well as their descriptions and thoughts about privacy. Responses to these initial interviews have helped to develop the questions for the second set of pilot study interviews which was conducted soon after the four week tracking period. The final interviews aimed at learning about participants' experiences of taking part in the tracking study and any thoughts or potential concerns regarding privacy.
The pilot study proved useful to familiarise the researcher and the participants with the concept of location data. The pilot interviews provided valuable leads to be pursued later on in the research project in more in-depth interviews.

3.3 Interviews

The interviews for this study were conducted in three phases: the first phase consisted of eight explorative interviews for the pilot study and the second phase consisted of five interviews, after which the survey was initiated. The reasons for conducting the survey at this point was for one part to allow time to reflect on how to approach the next set of interviews and for the other part to learn about individuals' awareness and opinions regarding location data on a greater scale than it would have been possible with interviews. The third and last interview phase took place after the paper-based survey was completed.

Interviews can provide insights that are not available to researchers working with large survey samples and are known to be the most suitable approach when seeking rich data illuminating individuals' experiences and attitudes. Drawbacks are that interviews are very time-consuming to conduct and analyse. The interview questions for interview phases two and three were based on findings from the pilot study. The questions were asked in as non-directive a manner as possible to meet the study's principal aim of learning about the interviewees' perceptions. The data collection and analysis for this project took place in alternating sequences and was guided by the grounded theory methodology. This meant that the interviews were transcribed and coded immediately after they took place. Hence, initial findings from interview coding could help to shape the questions for subsequent interviews.

3.3.1 Sample design and ethical considerations

For the second and third interview phase, the participants were initially contacted informally, which was followed up by an email explaining the study's aims and the interview procedure. The email ensured participants about anonymity and confidentiality of data collected and informed them that the interview was recorded for transcription (see Appendix B - Email sent out prior to interviews). The interviews were recorded with a digital voice recorder and the files transferred to a PC for transcription. When transcribing the interviews, participants' names were replaced with code numbers. Participants of the pilot study were assigned the codes P116_F, P117_M, P118_F and P119_M. "M" indicates males and "F" stands for female. The codes for respondents of the second and third interview phase followed the same system, starting with number P131_F. In addition to the eight pilot study interviews, ten more in-depth interviews were conducted which were between 30 and 90 minutes in duration.

Respondents were selected based on initial findings. The pilot study had for example highlighted different types of mobile phone users and it seemed as if different types of users utilise their phone settings in different ways to regulate how others can get in touch with them (see section 4.2.8). Hence it was sought to interview male and female mobile phone users from different age groups and with different mobile phone contracts. A list of respondents, including demographic characteristics, can be found in Appendix F - List of Interviewees.

3.3.2 Interview preparation

The information sent out before the interview included some technical and legal background about mobile phone location data. The email did not make any references to potential impacts of data retention on civil liberties or privacy so as not to influence the respondents' views. The aim of sending out information prior to the interviews was to familiarise the participants with the subject area. This seemed necessary because early survey findings showed that the majority of people had either not heard of location data or were not sure about the details.

3.3.3 Development of interview questions

The interview questions were based on initial findings from pilot study and survey and the following themes were addressed (see Table 3.1, below). Appendices D and E provide a detailed list of interview questions.

Table 3.1: Themes of interview questions for second and third interview phases

Theme	Notes about question
Mobile Phone	Mobile phone usage and habits in everyday life situations.
Privacy	An open question as to what privacy means to the interviewee. Deliberately trying to avoid mentioning any categories of privacy known from the literature.
CCTV, Loyalty Cards	Do interviewees perceive these as privacy invasive?
Phone as tracking device	Referring to technical and legal facts of mobile phone location data that were sent out prior to the interview. - Is the interviewee aware of location data before this study? - Are any issues or concerns raised?
Government & mobile phone service provider	- What is the participants' opinion towards storage of communications data (and its availability to government)? - What else is mentioned in this context? Regarding government, regarding data retention?
In addition to these themes, participants mentioned terrorist attacks, current politics and ID cards.	

The interview questions changed and improved over time, influenced by codes and categories developed for previous interviews. For this reason, two sets of interview questions are shown in the appendices: Appendix D - Interview questions March 2005 and Appendix E - Interview questions December 2005. The second set of questions was guided by Kathy Charmaz' approach to GTM, particularly her chapter on how to phrase interview questions to allow respondents to express their views without constraints (Charmaz, 2006). For example the question 'Have you ever heard of mobile phone location data before taking part in this study?' was changed to 'What do you know about mobile phone location data?'. A question mentioning consumer loyalty cards and the storage of personal information by commercial companies was removed after the second interview phase. The reason for this was

that initial interview findings and the survey showed that respondents did not perceive this area as related to privacy.

3.3.4 Use of software for data management and analysis

Weitzman (2000) advocates the following benefits of using software in research projects: writing up, editing, coding, storage, search and retrieval, data 'linking', memoing, content analysis, data display and graphic mapping. However, he warns of 'false hopes and fears', pointing out that no software will be able to actually carry out the analysis process for the researcher. Software can support the research process but ideas and intellectual efforts have to come from the human being conducting the research and analysis.

For this study a word processor, Microsoft Word, and the qualitative analysis software NVivo were used to support the analysis and to help manage the interview data. The computer was utilised as efficiently as possible to reduce the amount of time spent on organising data and findings, to increase the speed of tiresome tasks, resorting the material and redefining codes. Qualitative analysis software facilitated following potentially promising analytic routes but also enabled these routes to be discontinued with ease. Dynamic and real-time representation of the findings considerably assisted reflection on data and connections between the data.

3.3.4.1 Transcribing interviews and importing into NVivo

The use of the NVivo software has significantly facilitated the process of organising, re-arranging and managing the considerable amount of data. For example, after coding the interviews in NVivo, all passages assigned to a specific code could be viewed on screen and printed. In the same manner, searches for specific text strings could be conducted across all interviews and relevant paragraphs containing the search string could be compared on screen or printed. The interview transcripts were formatted in a particular way in Microsoft Word to facilitate importing the transcripts into NVivo. This meant for example, that the interview questions were assigned a 'Heading 1' format. When importing the transcript into NVivo, this resulted in the questions being displayed in the content panel in the NVivo explorer. Hence when selecting a question, it was possible to jump to this section in the interview transcript. Furthermore, meaningful information *about* the interview was placed into the first two paragraphs of each transcript. This enabled this information to be automatically put into the properties of the interview document when importing the interview into NVivo.

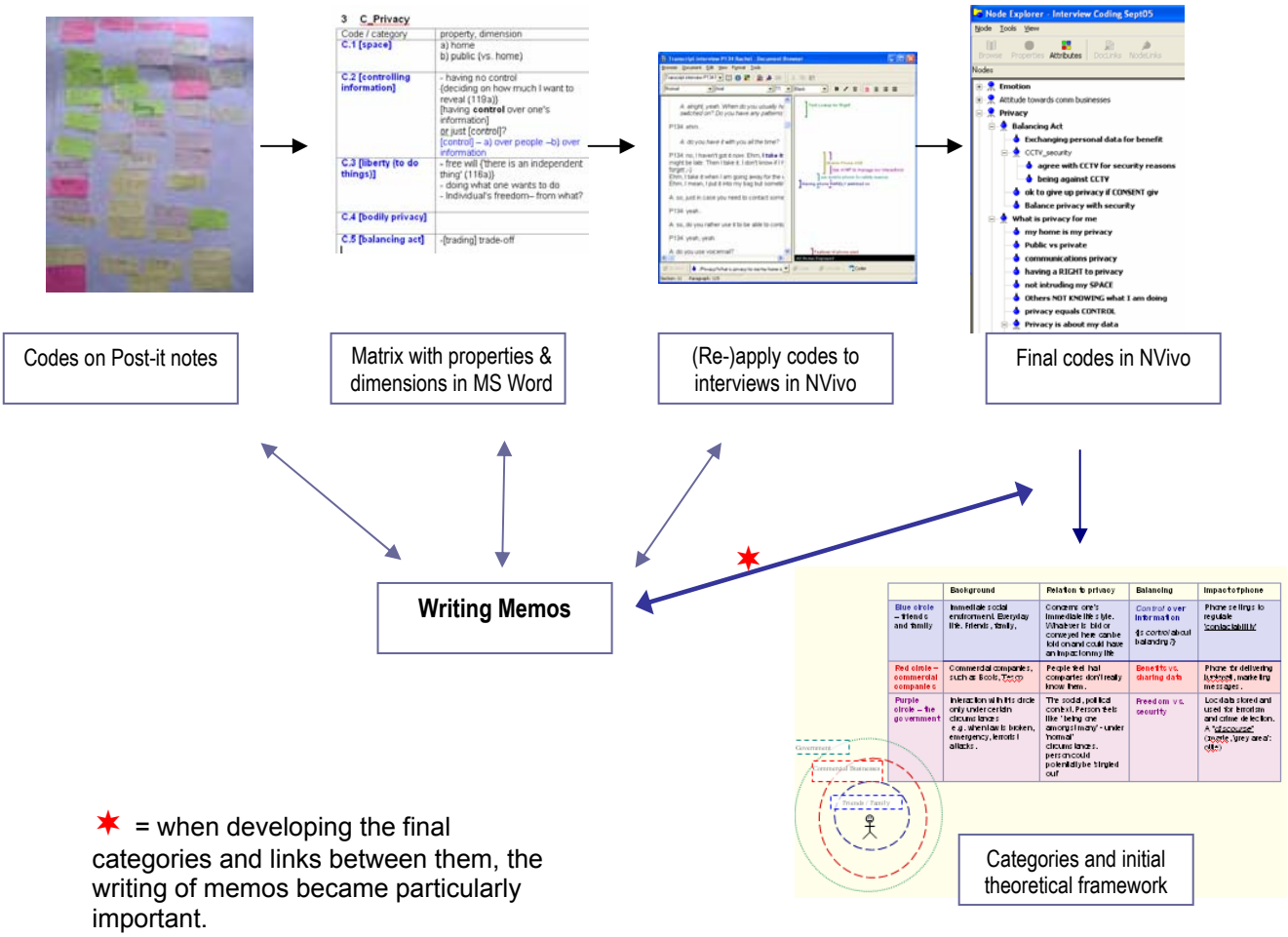
The appropriate formatting of the interview transcripts from the beginning helped to organise the data efficiently and thus facilitated the analysis of the interviews. In addition, by using the NVivo software much tedious and time-consuming work for managing and resorting the data could be avoided which freed time for more meaningful tasks, such as analysis and interviewing. Different sets of interviews could be assigned with different colours in NVivo for easy distinction.
An advantageous feature of NVivo is that the software keeps a log of all data that has been entered, which means that all codes and memos are automatically assigned a date and time stamp. This feature helped to trace the development of codes. After coding the interviews in NVivo, all passages assigned to a specific code could be viewed on screen and printed. In the same manner, searches for specific text strings could be conducted across all interview sets.

3.3.5 Interview coding

The first set of interview transcripts were coded with the help of the qualitative analysis software NVivo, which however did not prove to be the most beneficial approach (see section 4.1.6.1 Some initial concepts not confirmed). After setting aside several months for the survey, a fresh and more suitable approach to the analysis of interviews was adopted. This time interview codes were not devised on screen with help of software but with pen and paper. Following the GTM guidance on coding (see section 3.1.1.1), the researcher worked through each of the transcripts and used line-by-line coding to take note of themes and phenomena on the margins. The codes were not devised strictly microscopically and some more abstract categories came into view; some codes were very close to the interviewee's accounts and others more abstract or conceptual. Keywords and phrases were noted on differently coloured post-it notes and stuck onto a blank A2 flip chart sheet (see Appendix I). The post-it-notes were arranged in a logical order on the paper sheet. As more and more interviews were coded, this sheet started looking less like a random collection of labelled post-it notes but more like a brain storm map or a tree where branches of thought grew from certain categories. Memos were written throughout this exercise to keep track of thoughts and ideas regarding the data analysis.

This system of creating codes, combined with reflection was maintained for coding all interviews. At the end of this coding exercise, three A2 sheets were covered with post-it notes containing categories and codes. In addition, a matrix had been

devised, which held codes, properties and dimensions, as well as some comments and quotations. This list of codes was revised continuously as more interviews were coded. The codes were modified and verified by being applied to further interview transcripts but stayed alike for the most part. Subsequently, the codes were keyed into the NVivo software to allow searching the interviews, re-sorting of material and consistent redefining of codes in order to support the analysis process.
Figure 3.6, below, shows a summary of the coding process. More details about this analysis process are discussed in the subsequent findings and analysis chapters. Appendix J provides a summary of the development of codes.



★ = when developing the final categories and links between them, the writing of memos became particularly important.

Figure 3.6: Graphical representation of coding process

3.3.6 Memoing to develop and clarify categories

The extended coding process, as described in the previous sections, has facilitated reflections on codes and categories, which were captured by writing memos (for examples of memos see next chapter, section 4.2.2 Situational map as a memo to consider wider social context). The memos were consulted when establishing links between categories and setting up the initial theoretical framework. The following chapter details how initial codes have developed into focused codes and finally to abstract categories (section 4.2 Development of categories based on interview data). The writing of memos ('memoing') was particularly useful as this helped the researcher to keep a note of thoughts without the pressures of having to immediately determine how ideas fitted within the overall research findings and analysis. Memoing allowed the freedom to jot down ideas so that these could be sorted, categorised or discarded at a later point in time. The writing and reflecting on memos has been a crucial step in the development of the final categories based on initial and focused codes. Some examples of memos and how they have influenced the analysis process are shown in the next chapter (for example section 4.2.4 Memo ‘Balancing security and privacy’).

3.4 Survey

A survey was conducted in form of a questionnaire and distributed after the pilot study and some further interviews took place. The survey complemented findings from the interviews and helped to obtain a better idea of individuals' opinions towards privacy and mobile phone location data. Additionally, the survey highlighted interesting cases which could be approached in further data collection stages and thus supported the purposive sampling approach of interviews. It could be understood as a weak point of questionnaire-based surveys that they only capture surface opinions, seeing that respondents will not necessarily report their beliefs and attitudes accurately. These are easier to identify in interviews, as also prompts can be used. In addition, the use of mainly closed questions in a questionnaire merely allows respondents to choose between a limited number of responses (Robson, 2002). However, some of the respondents of this survey have overcome this limitation by making comments on the questionnaire’s margins to express further opinions and thoughts. A significant advantage of using a survey for this study was to collect larger amounts of data in a shorter time scale than would have been possible with interviews.

3.4.1 Sample design and ethical considerations

It is hardly ever possible to survey the entire population to be studied and for this reason sampling techniques need to be employed. A representative sample produces results which can be used to formulate generalisations. However, this can only be achieved by using probability sampling where the likelihood of the sampling unit - in this case an individual - to be included in the sample is known. The sampling population for this research project consisted of British residents older than 15 years, as the survey was not designed to explore the views of children. A representative sample was not chosen as it had not been possible to obtain a large enough random sample due to time and monetary constraints. For these reasons purposive sampling, a form of non-probability sampling, was used. Participants were not selected randomly but judged to be of interest to the researcher, which should not be understood as a limitation since the survey was designed as an explorative study. In addition, this approach tied in with the sampling procedures common in studies using grounded theory methodology (see section 3.1.1).

The questionnaire was distributed to individuals of different age groups, diverse professional backgrounds and users with different types of mobile phone contracts. The sample size of 477 respondents was deemed to be sufficient for an explorative survey and provided an overview of participants' opinions at the time of data collection. Statistical measures such as confidence intervals could not be produced as the sample was not a probability sample and the survey did not have a defined population. Ethical guidelines were carefully followed when collecting the survey data: all data were treated confidentially, which was explained to the respondents together with the aims of the study. Respondents were free to fill in their name on the last page of the questionnaire if they were interested in taking part in a follow-up interview. The section revealing individuals' names could be handed in separately from the questionnaire responses to ensure anonymity.

3.4.2 Pilot testing of survey

The questionnaire was thoroughly pilot tested before dissemination to uncover flaws and potential causes of confusion, such as misleading questions that could potentially result in invalid responses. For the pilot test 15 questionnaires were distributed to friends and other well-known contacts to verify feasibility and compliance with objectives set out by the overall study. The following steps were undertaken to pilot test the questionnaire:

1) Develop questions
The survey questions were based on interview questions from the pilot study. Five questionnaires were distributed to friends and colleagues, who were informed that the questions were developed for a survey. Their comments and feedback was used to modify some of the questions.

2) Pilot testing
Ten revised questionnaires were distributed to other friends and colleagues and their feedback helped to develop the final version. The number of questions was reduced from 23 to 20 and the layout was condensed, so that the number of pages could be reduced to four instead of seven pages.

3) Pilot analysis
Frequency tables for the responses to each question were generated to obtain an early impression of the results. This trial analysis ensured that the survey would fulfil the survey's aims and yield data valuable to the overall study.

3.4.3 Changes undertaken after successful pilot testing

After the initial analysis of pilot data, some changes in questionnaire design and coding were undertaken. The most significant change was to amend the answer choices of question 15 “Have you heard of mobile phone location data before taking part in this study?” to:

- I have heard of location data from the media and other sources, but I am not exactly sure about the details
- Yes, I know what location data is and how it works. I could explain it to a friend
- No, I have never heard of location data

The reason for this change was that the previous answer choices were not meaningful enough, as the questionnaire merely asked whether people had 'heard of' the data and if yes from which sources. However, it was acknowledged that it would be more important to learn how much respondents would consider themselves to know about the subject. The drawback of these answer choices was

that respondents had to use their own judgement. Nevertheless, it was not seen as appropriate to examine participants' knowledge, since it was more important to gain respondents' trust to enter into a dialogue. An additional change regarding question 15 concerned the layout. This significant question was moved to the bottom of the page, so that the box providing explanations about location data would only appear on the subsequent page of the questionnaire. Hence, this forced respondents to make a judgement of their awareness of location data before being presented with further background information on the subject area. Appendix L contains the final version of the questionnaire.

3.4.4 Distribution of questionnaires

The survey was disseminated in two formats, paper-based and online via the internet; the majority of questionnaires were distributed paper-based. Initially the survey was given to individuals working and studying at Leeds Metropolitan University, ranging from respondents with an academic background (lecturers, post- and undergraduate students) to administrative, cleaning and security staff. Friends, personal contacts from various leisure activities and colleagues from part-time jobs were also invited to fill in the questionnaire. In addition, acquaintances working in different professions (landscape architect, engineer, manager in a bus company) were asked to distribute approximately 10 questionnaires each at their workplace, sports club or family. This distribution method could be seen as a form of snowball sampling, which ensured access to social groups beyond the researcher's immediate social circle and made it possible to collect data across a diverse population. A known limitation of the sample for this study is that unemployed, unskilled or manual workers were only included marginally.

It was acknowledged that researcher's bias could have occurred when selecting participants. Response rate and quality of survey data was very high due to the questionnaire distribution on a personal basis. An additional benefit of this approach was that respondents could receive help with completing the questionnaire if necessary. Only a few people refused to fill in the questionnaire, mainly due to time constraints, and one person did not want to participate as she perceived questionnaires as an invasion of her privacy. It is acknowledged that due to the chosen non-probability sampling method, the number of non-respondents and their reasons for not taking part in the study could not be known.

3.4.5 Online survey

In addition to the paper-based version, an online version of the questionnaire was published on the internet on a website developed by the researcher (http://www.locationprivacy.org). The survey questions were identical for both distribution media so that the results could be pooled. An online survey was seen as a convenient way to collect additional data with minimum involvement of the researcher in data collection and analysis. Results of the survey were automatically gathered in a database and could be downloaded in form of tabular data which then could be imported into Ms Excel. Advantages of electronic surveys include being able to direct respondents to particular sections of the questionnaire, depending on the way they have answered previous questions. Respondents can be automatically prompted when they provide an invalid response, such as selecting several tick boxes when only one should be marked. However, electronic surveys also have distinctive technological, demographic and response characteristics which were to be taken into consideration for this study. For example, only individuals with computer and internet access were able to fill in the survey. To account for these differences data from the electronic survey was stored and analysed separately from the data collected by the paper-based version. However, a comparison between the responses from both distribution media showed that results were similar (see section 4.3.1).

3.4.6 Email as distribution medium

Email was planned to be used as a distribution medium for the survey but discarded due to particular problems to this approach. Two alternative methods for using email to distribute surveys were considered; firstly, to send the survey as an attached word document, and secondly to include the questions in the email body. However, for the first option it would have been necessary for the respondent to download the attachment, complete and save it and then re-attach it to the email to send it back to the researcher. This is a rather cumbersome process and if any of these steps is not followed correctly, the survey is returned blank. The second option would not have allowed the researcher to control how the questions are displayed, as this depends on the respondent's email programme. For these reasons the use of email was restricted to distributing the questionnaire's website link and to contact respondents.

3.4.7 Question design and coding

Questions were worded carefully and avoided long and ambiguous, leading, biased questions, as well as jargon. The following question types of questions were used:

Numerical rating

A Likert scale from 1 - 6 was used. The reason for using an even number of options was to not allow non-committal answers. In the data analysis, each statement was assigned a separate variable.

8. How important is your phone to you on a scale from 1 to 6?

My phone is VERY IMPORTANT to me. It would be difficult to live without it.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐	**NOT IMPORTANT at all to me.** I could live without it.

Multiple choice

Require respondents to choose just *one* response from a list of alternatives. Only one variable per question was necessary in the data analysis.

14. Giving up some privacy is necessary to fight terrorism and crime

Agree ☐ Disagree ☐ Don't know ☐

Check lists

List a set of items of which respondents select those that apply. Each statement was assigned a separate variable in the data analysis.

18. In your opinion, what would be good uses for location data? [Select *all* that are appropriate]

Solving crime	☐	Employers to track their employees	☐
Preventing acts of terrorism	☐	Emergency services	
For parents to track their children	☐	(e.g. rescue, ambulance, fire brigade)	☐

Open questions

Open questions allow respondents to formulate their own statements and can lead to unexpected responses. Nevertheless, open questions are more difficult to analyse and take respondents longer to respond. For this reason only one question of this type was included.

9. What comes to mind when you think about the term 'privacy'? [*Keywords* are fine]

Non-committal responses

The survey questions raised many issues which respondents might not have thought about before taking part in the study or might not hold an opinion. Hence, alternative responses such as 'don't know' or 'no opinion' were provided where appropriate. It would create false and unreliable answers to force the respondents to express an opinion. Some see the danger in providing these options that some respondents might select them out of laziness (Converse and Presser, 1986 in DeVaus, 2002). Therefore, alternative responses were always the last one in a list of options (see Appendix L).

3.4.8 Coding missing responses

In every survey there will be missing data occurring for different reasons, which needs to be recorded and coded in a similar way to valid responses. In this study, different codes were given to different types of missing data. The following types of non-responses were identified:

1) The respondent has not responded to a question. The reason might have been by choice or simple overlooking of the question. The code given was ‘9’.

2) The respondent was not required to answer this question. After responding to the question ‘Do you own a mobile phone?’ individuals who did not own a phone would proceed straight to Section B ‘Privacy’. The missing responses in Section A ‘Mobile Phone’ was coded with an ‘8’ to distinguish those from other missed responses (see above).

3) Response was invalid, e.g. where only one answer was required but the respondent ticked several responses. However, this was only the case with one questionnaire and therefore in this case was assigned a ‘9’.

3.4.9 Data entry

The survey data was firstly entered into an Excel spreadsheet and then imported into the statistical analysis software SPSS (Statistical Package for Social Scientists). The reason for using two different software packages was that Excel would automatically update graphs showing the frequencies of responses as survey data was entered. This gave early impressions and ideas about the data and helped reflecting on findings at an early stage. Another reason for entering the data first into Excel was that there was no character limit for variables, which was convenient for open question and comments. Afterwards, data was imported into SPSS to facilitate advanced analysis of data, such as correlations between variables. In addition, SPSS could help to prevent false entries, as data ranges could be set, so that for example no number greater than 6 could be entered for a question.

3.5 Analysis of findings

Data collected by pilot study and survey were compared to the grounded theory categories identified in the interviews in order to support the analysis of findings. This process of triangulation between qualitative and quantitative data was used to confirm and validate the findings.

The interplay between induction and deduction, in other words between data collection and interpretation, was another process of validation of findings but also part of the theory development (see section 3.1.1). In what is known as a process of abduction, the interpretation of observed data to the best explanation helps to form a tentative theory, which then needs to be confirmed or disconfirmed with help of further data collections and analysis. This procedure is repeated until the best, the most plausible interpretation of data is found (Charmaz, 2006; Haig, 1995). The findings from empirical data were compared to the reviewed literature, as described in Chapter 5, which then lead to conclusions and recommendations (Chapter 6).

3.6 Chapter summary and conclusion

This chapter has introduced and discussed the choice of grounded theory methodology as a suitable research methodology for this study. The continuous generation and long-term retention of mobile communications data are inherently related to the every day transactions of every mobile phone user. The views of mobile phone users are necessary to be captured as information about their lives is at the centre of debates around data retention.
A grounded theory has been developed to provide an explanation for the phenomenon under study: the relationship between mobile phone location data and individuals' perceptions of privacy in the UK. The theory can be categorised as ‘substantive’ as opposing to a ‘formal’ theory, since the collection of data and their interpretation focus on the explanation of a particular area. The chapter has in great detail explained each of the three data collection phases, including sampling and ethical considerations. A mobile phone location tracking pilot study, a survey and a series of interviews have been conducted to learn about individuals’ perceptions of privacy in relation to location data. The iterative cycle of data collection and analysis is an essential element of GTM and has helped to shape the on-going data collection.

The following chapter, Chapter 4 - Presentation of Findings, discusses in detail the findings of all three data collection phases, pilot study, interviews and survey.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 4 Presentation of Findings: Mobile phone location tracking Pilot study, Interviews and Survey

This chapter provides a detailed account of the findings from the three empirical data collection phases. Accordingly, this chapter is structured into three parts; the first part discusses findings from the pilot study, the second part focuses on the analysis of the in-depth interviews and the third part presents findings from the survey. Grounded theory codes, memos and visual demonstrations of ideas provide an insight into how the final grounded theory categories were developed. The methodology for this study, which had been discussed and explained in the previous chapter, has guided the data collection as will illustrated in this chapter. The focus of this chapter is to present and discuss the results of the three phases of data collection, a comparison of those findings with the relevant academic literature will be provided in the following Chapter 5.

Relationships between data collection phases

The following methods were used to collect empirical data: mobile phone tracking, interviews and a questionnaire. As explained in the previous chapter, Chapter 3 - Methodology, data collection and analysis took place in several stages and in alternating sequences (see Table 4.1). This was an important and beneficial element of the grounded theory methodology.

Table 4.1: Data collection and analysis phases

Time line	Data collection	Data analysis	Analysis method	
August and September 2004	*Interview phase 1* - Conduct and transcribe 2 x 4 pilot study interviews - Track location of 5 mobile phones over 4 weeks	Initial codes	- Analyse data with content analysis matrix - Open coding with NVivo software	
March 2005	*Interview phase 2* - Conduct and transcribe 5	Focused codes	- Focused coding with post-it notes and	Memo

	in-depth interviews		NVivo software	writing
April to September 2005	*Survey* - Develop and test pilot questionnaire - Distribute questionnaires paper-based and online, N=477	- Data entry into Excel - Data analysis with SPSS (frequency tables, graphs and cross-tabulations)		
October and November 2005	*Interview phase 3* - Conduct and transcribe 5 in-depth interviews	Focused codes	- Focused coding with NVivo software	
September to December 2005	Develop final categories			

To begin with, eight pilot study interviews were analysed with the help of a content-analytic summary table, as shown in Appendix G. Four interviews were scheduled to take place before the tracking period in which the geographical location of the participants' mobile phones was requested once a week. After this four week period, each of the four participants was interviewed again. The results of this first interview phase are illustrated in the first part of this chapter (section 4.1.2). Following this, the pilot study interviews were analysed with help of the grounded theory methodology. A large number of initial and tentative codes were assigned to every interview. Subsequently, two more sets of interviews, representing interview phases two and three, were conducted and assigned with focused codes. In-between the latter two interview phases the questionnaire was distributed, for the most part paper-based but also via the internet. The results of the survey are discussed in the final part of this chapter (section 4.3, Presentation of survey findings). Memos were written during the entire process of collecting and analysing data, as this facilitated reflection on the collected data. A number of memos are shown throughout the chapter to demonstrate their importance for the development of the final categories (see section 4.2 Development of categories based on interview data).
As described in Chapter 3 - Methodology, participants' names were replaced with code numbers to ensure their anonymity. Participants of the pilot study were assigned the numbers P116_F, P117_M, P118_F and P119_M. "M" indicates males and "F" stands for female. The codes for respondents of the second and third interview phase followed the same system, starting with number P131_F.

4.1 Mobile phone location tracking pilot study

The pilot study set out to achieve the following two aims: for one part to evaluate the practical aspects of location tracking and for the other part to learn about participants impressions. Therefore, the pilot study involved two data collection methods. At first all four participants of the pilot study were interviewed, followed by a four week period in which their mobile phones were located at different times once a week. The participants could not know when a location request for their mobile phone was submitted. This collection of mobile phone location data is discussed in part one of this section. Part two presents findings from the interviews and focuses on the participants' experiences with location tracking.

4.1.1 Part one: Mobile phone location tracking

Five mobile phones, those of the four participants and the researcher's mobile phone, were registered with a commercial mobile phone tracking service provider (see Chapter 3 Methodology, section 3.2).

The aims of the technical and procedural side of mobile phone location tracking were set out as follows:

Aim 1: Reliability of the mobile phone location service

- How well does the service work for four UK service providers (Vodafone, O2, Orange, T-Mobile)?
- Do all location requests bring results?
- Will the result be displayed within a reasonable amount of time, e.g. a few seconds?

Aim 2: Text message reminder

- How often and when do mobile phone users registered with the service receive text messages asking for their consent to be located?

Aim 3: Accuracy of tracking results

- What is the accuracy of the service?
- Are the results sufficiently accurate to identify the participant’s approximate location?

4.1.1.1 About the four pilot study participants

Both male participants (P117_M and P119_M) had owned their phone longer (5 and 9 years) than the female participants P116 and P118 (2 and 4 years). Two participants had signed up for monthly paid mobile phone contracts and the other two used pre-paid mobile phone contracts. All participants happened to own a black-and-white Nokia handset and all stated that they would usually carry their phone with them and have it switched on 24 hours each day. All participants used their phones for calls and text messaging, some as an alarm clock and some occasionally for games. Only the participant P119_M sometimes used WAP services, and he owned his mobile phone for the longest period of time in comparison to the others (for details see Appendix G - Content-analytic summary matrix for pilot study interviews).

4.1.1.2 Aim 1: Reliability of the mobile phone location service

Tracking results were supplied by the commercial tracking service provider for all five mobile phones which were registered with the four UK mobile phone providers: Vodafone, O2, Orange and T-Mobile. Results of location requests were provided almost instantly after submitting the request and were reasonable accurate (see Aim 3, below).

Only a number of location requests for one of the two mobile phones using the T-Mobile network (P116_F's phone) did not provide immediate results. For this participant, three out of four location tracks did not succeed on the first attempt. This was especially paradoxical, as on one occasion P116_F had been contacted on her phone shortly before a location request, which meant that she had her phone switched on and was receiving a network signal.

4.1.1.3 Aim 2: Text message reminder

A few minutes after registering the participants' phones with the tracking service provider, each phone received an activation text message. This text message contained a password which the participants had to forward to the researcher. Those passwords were then entered on the researcher's account at the tracking service provider's website. Shortly afterwards the participants received the following text message "You have authorised a.gorra@leedsmet.ac.uk to locate your phone. To stop call 0870XXXXX".

From now on the participants' phones could be located 24 hours a day. The same authorisation text message was received by all participants 4 and 8 weeks after the initial registration but then ceased to be received by all registered phones. The potential reason that this text message ceased to be sent might have been that no further tracking request were submitted after the pilot study ended.

4.1.1.4 Aim 3: Accuracy of results

The precision of the tracking results varied widely and mainly seemed to depend on the size of the cell in which the user stayed when the location request was submitted. The best precision with a radius of 500 metres was achieved in Leeds city centre (see Figure 4.1), and the least accurate result was found near the sea side and with a radius of accuracy of 11km (Figure 4.2). Urban city centres have more mobile phone users and hence more masts and therefore smaller cells than places in the country side (see Chapter 2 - Part 2: Mobile phone location data, section 2.2.1.2).

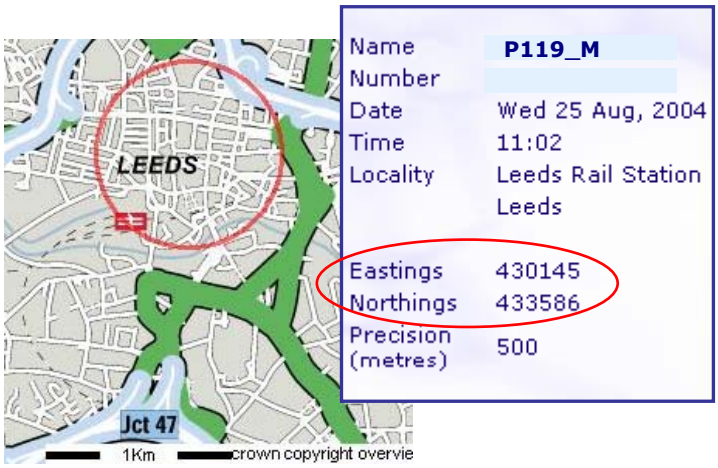


Figure 4.1: *Most* accurate track (P119_M)

In addition to the precision in metres, “Eastings” and “Northings” were provided for each location request, which indicate coordinates on Ordnance Survey maps (see Figure 4.1). Those coordinates corresponded to the centre of the circle shown on the map and were for the majority of tracks very close to the participants' actual position. For an example, see Figure 4.1 above, which shows participant P119_M's location *supplied by the tracking provider*.

Figure 4.2: *Least* accurate track (P116_F)

This location can be compared to the participant's *actual location* determined by his postcode at time of tracking (see Figure 4.3). In Figure 4.3, below, the blue circle indicates the area provided by the tracking provider. The red circle shows participant P119_M's actual location.

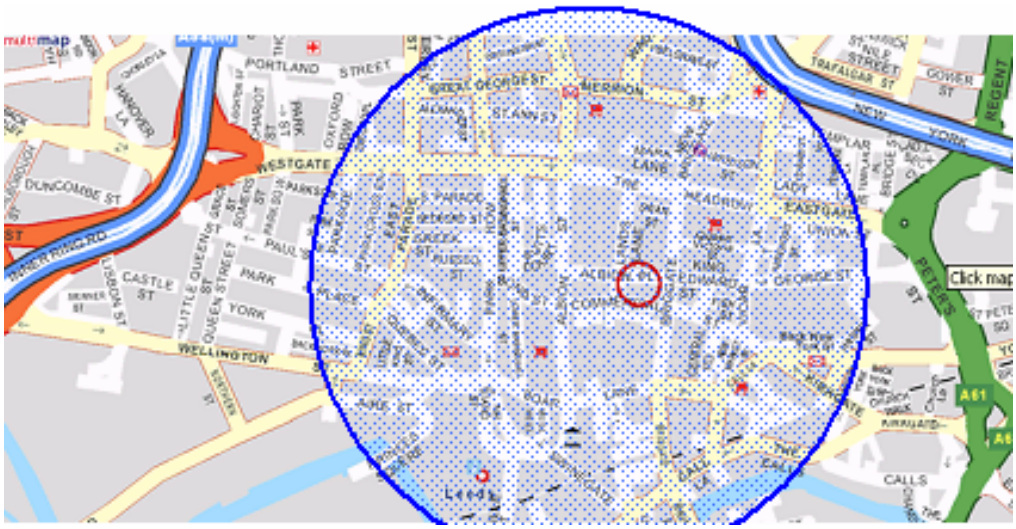


Figure 4.3: Actual location of P119_M

Name	P117_M
Number	
Date	Tue 10 Aug, 2004
Time	19:57
Locality	Facit
	Rochdale
Eastings	389905
Northings	415289
Precision (metres)	2237

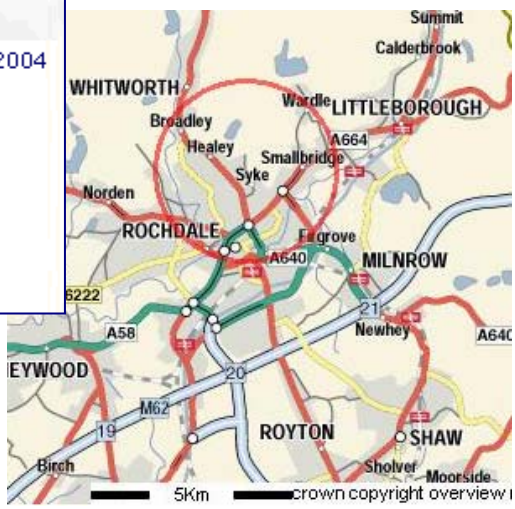


Figure 4.4: Location of P117_M, 11th August 2004, 8pm (radius 2.237km)

At first sight, the accuracy of the majority of location tracks seemed disappointing. The average precision of the 16 location requests was 2.271 km for the radius of the circle in which the participants' phone was located. This means that the area in which participants could have been at the time of tracking can be calculated with 16.2 km^2. Figure 4.4 shows a location track with the approximate average precision to illustrate the size of the area. The red circle indicates the area in which the mobile phone user P117_M might have been when the location request was submitted.

Figure 4.5 compares P117_M's actual location (red circle) to that provided by the tracking service provider (blue circle). His actual location was identified with the help of the post code supplied by the participant in the final interview. This comparison shows that the average precision of location tracks within approximately 16 km^2 fails to identify the precise location of the mobile phone user but instead only gives an indication of geographical location at the time of tracking.

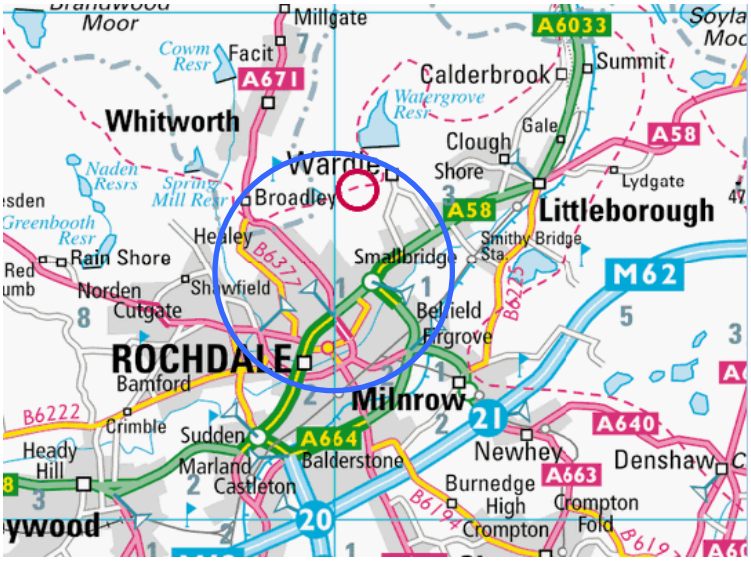


Figure 4.5: Actual location of P117_M

4.1.1.5 Summary Part 1: Mobile phone location tracking

The majority of location requests were successful, with a small number having to be repeated, possibly due to network problems (see Aim 1). Overall, the tracking results have been acceptable in terms of indicating the participants' geographical location. For all 16 tracks, the participants' actual locations have been within the circle marked by the tracking service provider. On the one hand, the circles have indicated a large area, on the other hand however, in nearly all cases the participants' locations have been near the middle of the circle, as indicated by the Eastings and Northings (see Figure 4.2).

In addition, even though the tracks were not able to show the exact location of the participant at the time of the track, in the form of a street name or postcode, this information could often be deduced. Assumptions could be made about participants' specific whereabouts based on other information known about the participants. These assumptions were mostly confirmed in the final interviews when the participants were questioned about their actual locations at the time of tracking. Hence, it can be argued that the current precision of the tracking system is sufficient for personal purposes, such as parents identifying the whereabouts of their children or employers interested in their employee's current location within a particular number of company sites. It could be claimed that the bigger the capture area in which those being tracked could be, the more valuable are location tracking results based on a postcode. For example, the participants of this study mostly stayed within the Leeds area during the four week tracking period. However, if they would have travelled all over the UK to visit a particular number of sites, the results would have indicated their approximate area and hence the nearest site could be identified.

The tracking service provider utilised for this study appeared to make use of the cell-of-origin tracking method but it is technically possibly to determine a mobile phone handset's location with a much higher accuracy (see Chapter 2, section 2.2). An interview with the director of the tracking service provider could not provide any clarification, as he did not want to convey any technical details about their method of location tracking for reasons of business competition. This may indicate that the geographical location of mobile phones could constitute a worthwhile business opportunity and *may* be increasingly used commercially in the future (see also section 2.2.3 for existing location-based services).

4.1.2 Part two: Pilot study interviews

The pilot study interviews aimed to learn about the participants' awareness of issues relating to mobile phone location data, such as

Aim 1: Awareness and attitudes towards mobile phone location data
Aim 2: Geographical location and privacy
Aim 3: Participants' definitions of privacy
Aim 4: Potential influences of having their location identified on participants' behaviour and regarding given scenarios
Aim 5: Participants' concerns regarding misuse and storage of location data
Aim 6: Privacy in relation to CCTV and loyalty cards

The pilot study interviews were conducted in two stages: one interview with each of the four participants was conducted before and one after the four week mobile phone tracking period. Interview aims 1, 2 and 3 were addressed in the first interview and aims 4, 5 and 6 were addressed in the interviews after the tracking period.
The interview data had been arranged in content-analytic summary tables to condense the data and to be able to compare the respondents' statements for each question (see Figure 4.6, below). Each of the interview aims is discussed below and the complete content-analytic summary tables for all pilot study interviews are shown in Appendix G. Appendix H provides the complete transcripts of all interviews.

4.1.2.1 Aim 1: Awareness and attitudes towards mobile phone location data

Both female participants stated that prior to this study they had not been aware about their mobile phones transferring information about their approximate location to the mobile phone service providers. Both male participants explained that they had heard about location data before the study, such as from TV programs dealing with crime. None of the participants was aware of the legal requirements of mobile phone service providers to retain communications data for several months. All participants agreed that access to their location data should be granted to police and other security services. They also stressed that the information should not be used for commercial reasons. Regarding the ownership of location data, only one participant (P117_M) claimed he wanted to have access to this data and compared it with one's credit history, which is accessible against a small fee (see Figure 4.6, below). P119_M suggested that "the people who generate it should look after it",

which for him were the mobile phone service providers. Some of the comments suggested that mobile phone location data is not seen as very personal or a potential threat, as P119_M explains: "I can't see it being used against me for anything".

	P116_f	P117_m	P118_f	P119_m
Q6: Who should own and have access to location data	I can understand police having access to it and owning it. And I don't really think anyone else should.	I think me for a start, because I think that people withdrawing information like this, I would want access to it. I don't know if they do but I know that, things like credit history, you can get a history for it and maybe an idea of getting through to that. (...) once you store these things, you know it could be kind of like misused quite easily and it is not necessarily in a big way, maybe in little ways. ... So, I don't know it depends, you wanted it to be regulated properly.	Like home office, people involved in security, Government And police.	the people who generate it should look after it, it's their data. "who's that?" the service providers. Unless the government wants to do a bit of centralisation and look after it themselves but I can't imagine it because they probably come up with system that crashes. Ehm, Access. Police, anti-terror, all that. Security services what you call them. Not the army because they are a bunch of tossers.

Figure 4.6: Extract from the content-analytic summary table

Regarding the storage of data, all agreed that the police should be allowed access to mobile phone location data. And when asked in the final interview about who they would trust to store their location data, three out of four participants stated that they would rather believe in the service providers to keep the data safe than the government. In addition, P116_F mentioned that she would only grant powers to the police to distribute location data. P119_M expressed the opinion that judges should be the ones to decide about dissemination of data.

4.1.2.2 Aim 2: Geographical location and privacy

In the initial interview, all participants were invited to talk about their thoughts regarding their geographical location in relation to privacy. Two participants (P118_F, P119_M) did not seem to be concerned at all about information revealing their geographical location because they "would not do anything wrong". After the tracking period, P119_M stated that having his mobile phone tracked did not affect his behaviour and for this reason location tracking was not an invasion of his privacy. P118_F stated that as long as she was in a public space, everybody could see what she was doing anyhow. She explains "what we do in public is not private (...) privacy is only inside my house" (P118_F). However, both P116_F and P117_M mentioned that they would find it "very intrusive" and would "feel

uncomfortable" if their location would be constantly recorded and both stated later on that they valued privacy even though they did not have anything to hide.

4.1.2.3 Aim 3: Participants' definitions of privacy

The descriptions of privacy in the participants' own words largely corresponded to concepts identified in the privacy related literature, such as territorial privacy, bodily privacy (see section 2.1.2). P116_F said privacy would be hard to define "because it does mean so many different things these days". Two participants (P118_F, P119_M) focused in their description of privacy on their personal space or territory. "you should have a reasonable expectation of privacy in your bedroom" (P119_M), "Anything out of my house, there is no privacy there" (P118_F).
The other two participants, P116_F and P117_M also talked about personal space but did not see it in restrictive terms of territorial boundaries but rather related it to the concept of liberty. Both highlighted their desire to have "individual freedom (..) being able to do things legally that not everyone knows about" (P116_F) and "to get away with doing what I want to do without other people finding out" (P117_M).

4.1.2.4 Aim 4: Potential influences of having their location identified on participants' behaviour and regarding given scenarios

All participants said that they had forgotten that their phones were registered with the tracking service provider after the four week tracking period. This might have been the main reason why all four stated that the tracking study had not influenced their behaviour in those four weeks. In the final pilot study interviews, the participants were asked to comment on two imaginary scenarios related to their work place and their partner. All responses were very similar. The participants said that they would not object to their partner wanting to track their mobile phone but all raised issues of trust. Some mentioned that they would want to know the *reasons* as to why their partner would want to track them.
None of the four participants could imagine that if their manager tracked their work mobile phone, then this would have an effect on their behaviour. P117_M compared this to telephone and email logs, which some workplaces keep and said that as long as no one is confronted with those, employees just tend to forget about the potential of being monitored. P116_F, P118_F and P119_M mentioned that because they would not "do anything wrong", they would not be worried about having their location tracked at work. These answers related to another question in the final interview "Do you believe that people who have got nothing to hide should not worry

about their privacy?". P118_F and P119_M agreed with the statement, whereas P116_F and P117_M believed that they should have some privacy even though they would not have anything to hide. This seeming contradiction between the desire to have privacy (in life in general) but not necessarily expect it at the work place, is picked up upon later in the final grounded theory categories (see 4.2.9 Different areas relevant to privacy).

4.1.2.5 Aim 5: Participants' concerns regarding misuse and storage of location data

The female participants, P116_F and P118_F, articulated as the main concerns regarding the misuse of mobile phone location data that the data could fall into the hands of criminals. For example burglars would be able to identify, with the help of location data, when they would not be at home. Both male participants once more stressed that it was important for them to know the *reasons* for being tracked and whether under certain circumstances this data could possibly be used 'against them'. As P119_M explains "But I think it all depends why people are tracking, to be honest. And then you have to work out what is using it and what is misusing it". When asked if they would rather trust the service provider to keep their data safe or the government, all participants, except of P118_F who worked for the local council, stated that they would not trust the government but rather the service provider. The main reasons given for not trusting the government were security and data access issues and the majority of participants believed that the data to be handled more securely by the private sector.

4.1.2.6 Aim 6: Privacy in relation to CCTV and loyalty cards

None of the participants seemed to mind CCTV cameras recording their movements as the cameras were seen to offer benefits for society, such as security. In the same manner, the majority of participants did not perceive it as an invasion of their personal privacy when using loyalty cards, as they helped to save money. P118_F and P119_M pointed out that purchases took place in the public sphere and that this would not be private anyway. P116_F and P117_M, who seemed generally more conscious about privacy related issues, said that it would depend on the benefits received in exchange for personal data and that these benefits should be clearly communicated to the consumers up front. These statements can be seen as an early indicator of the Core category 'Balancing' (see section 4.2.4 Development of Core category 'Balancing).

4.1.3 Summary of pilot study interviews

All four participants expressed similar opinions during the interviews which could be influenced by the somewhat homogenous sample of respondents who were all aged between 25 and 35. However, this was known beforehand and accepted in favour of gathering early data. Nevertheless, although the sample only consisted of a limited number of four people, a range of privacy-related opinions could be noted. One male and one female participant (P118_F and P119_M) did not seem to be concerned at all about their privacy in everyday life "I don't think I have got anything to hide and I am not worried about it" (P119_M). Whereas the two other participants, P116_F and P117_M, felt a bit more conscious about this subject. As P116_F put it "even though I haven't got anything to hide, I still like the fact that I have got some privacy".

The use of location requests via a mobile phone tracking service provider was a useful way to make mobile phone location data more tangible. However, as all participants stated that they had forgotten about being registered with a tracking service provider, this approach ceased to be used for future interviews. The content-analytic summary table had proven to be useful to summarise the interviews but did not support an in-depth analysis. This confirmed the researcher's decision to utilise a different approach to guide further data analysis and collection. For this reason, the pilot study interviews were analysed again using the grounded theory methodology (see section 3.3.5). The pilot study interviews were coded and followed by further more in-depth interviews based on initial findings without tracking participants' mobile phones. A discussion of these early interviews in relation to the relevant literature will follow in Chapter 5 Discussion and Analysis of Findings).

4.1.4 False starts with initial coding in NVivo Software

In order to analyse the pilot study interviews using the grounded theory methodology, four pilot study interviews were coded with the help of the qualitative analysis software NVivo. However, this first phase of coding was not successful as over one hundred codes were assigned to only four short interviews and some codes had only been used once or twice. Figure 4.7 shows a list of codes that were devised at this stage. In addition, it seemed that some of the codes and categories were 'forced upon the data', as Glaser and Strauss would call it (Glaser and Strauss, 1967). In other words, some codes resembled themes from the literature and were not explicitly mentioned by the interviewees.

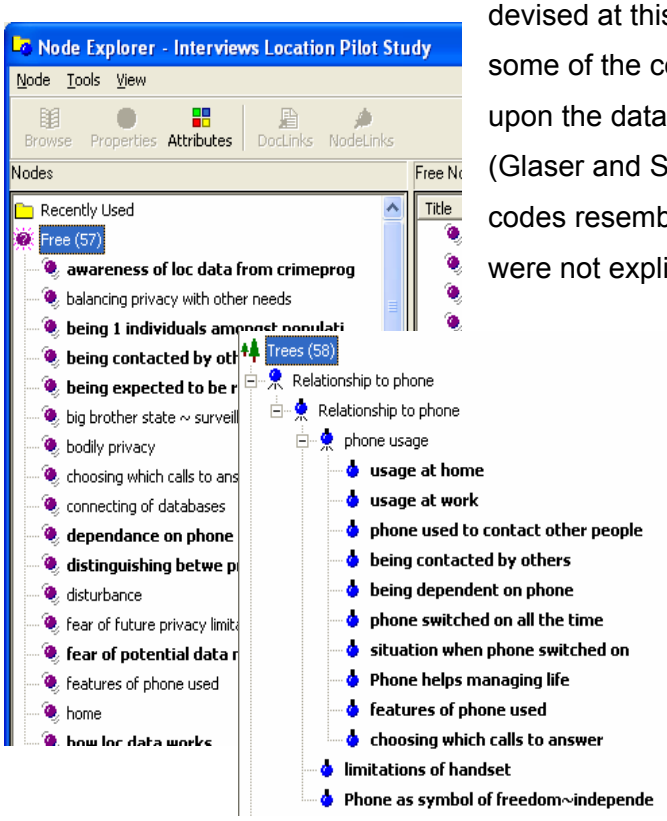


Figure 4.7: Initial interview codes in NVivo

Figure 4.8 below, shows some interview codes relating to privacy. These codes closely resembled categories of privacy commonly identified in the literature, such as 'territorial', 'bodily' and 'information' privacy (see Chapter 2, section 2.1.2). These reasons made it necessary to adopt a different approach for coding.

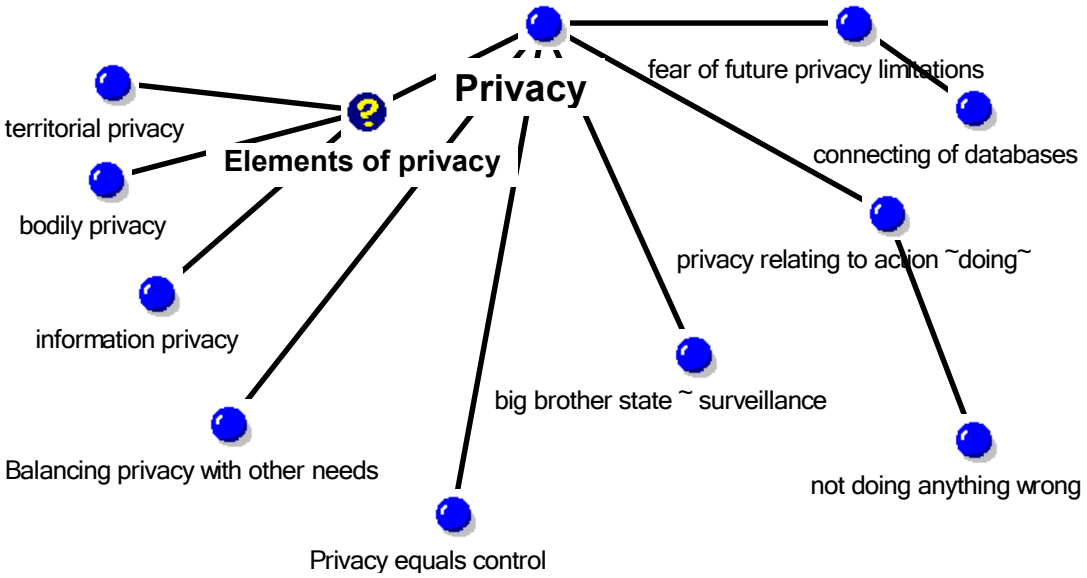


Figure 4.8: Initial NVivo model 'privacy' for pilot study interviews

4.1.5 Summary of initial coding of pilot study interviews

As explained above, the initial coding of the pilot study interviews did not prove to be very successful. This was mainly due to the large number of codes and due to numerous codes that seemed to have been influenced by the relevant literature. Nevertheless, the codes provided some initial ideas and were used as guidance for the next stage of interviews. Most of the initial codes could be grouped into the five categories: 'tracking', data sharing', privacy', 'data misuse/surveillance' and 'data safety' (see Figure 4.9). The numbers in brackets show how often the codes were used, for example "[2/4]" indicates that the code has been used in 2 out of 4 interviews.

These codes and categories later on guided the development of the final categories, including the Core category 'Balancing' (see section 4.2.4 Development of Core category 'Balancing').

Tracking	Data Sharing	Privacy	Data Misuse / surveillance	Data Safety
having forgotten about being tracked [4/4]	LD sharing ok as long as not affected	not doing anything wrong [3/4]	data being used against you fear of potential data misuse [2/4]	believe SP will keep LD safe [2/4]
motivation 4 tracking is most important [3/4] use of LD more important than tracking reason for tracking is important [1/4]	if there's a benefit I share my data [2/4]	experiencing privacy only at home [2/4]	talking about sinister gov body	more trust in SP than Gov 2 keep LD [2/4] (both male)
	more concern (about) current data than retention	not having anything to hide [2/4]	being under surveillance	worry of criminals misusing LD [2/4] (both female)
being tracked for justifiable reason [2/4] only share (general) data for a good reason [1/4]	no concern about long term retention	trusting partner to know 1's location [2/4]	being innocent but dragged into s.th.	believe Gov will keep LD safe
	wouldn't like partner tracking me	willing to share LD w friends, family [2/4]	big brother state ~ surveillance	believing that LD is in safe hands

Figure 4.9: List of initial codes for pilot study interviews

Another phenomenon that was highlighted by the initial codes was the mobile users' relationships to their mobile phones. This relationship varied from user to user and seemed to be related to the ways in which the phone was used, particularly to determine how others can get in touch with the user. Some codes around this area could be grouped together, as shown in Figure 4.10, below.

Receiving Calls

awareness (“not bothered whether I hear it ringing/bleep”)	choice of taking calls enhanced with caller-ID display	different ring tones for diff. situations

Privacy

Fear of future limitations of privacy; equals control; balancing privacy with other needs; not doing anything wrong
- public
- privacy relating to movement or action (doing)
- perceiving privacy as only being inside one's house
- not caring about doing something in public

Relationship to phone

- symbol of freedom
- dependence
- disturbance
- obsession
- phone use is voluntary (not forced upon)

Figure 4.10: Some initial codes for pilot study relating to mobile phone use and privacy

4.1.6 Verifying initial codes and categories

It is important for a sole researcher to verify all codes and categories that are assigned to interview data to ensure that they are applied consistently (Miles and Huberman, 1994). In order to verify the initial codes set up in NVivo in the first phase of coding, the researcher started afresh by open coding the pilot study interviews with a different method than before. The interview transcripts were coded with pen and paper, and following this the codes were transferred onto post-it notes. The post-it notes could be arranged in groups and this helped to identify patterns in the data. Afterwards, the codes were then entered into a Microsoft Word document together with some comments and finally transferred back into a new NVivo file (see Chapter 3, section 3.3.5 and Appendix J).

A comparison between new and previous assigned codes helped to clarify whether the codes were reliable and truly represented the empirical data. The comparison showed that past and present codes were similar to each other. However, initial codes were often either too narrow, too close to the interviewees' exact words or seemed to mirror themes known from the literature. Hence, the benefit of re-coding the interviews consisted of reconfirming and refining the codes. Memos were used to reflect on changes in codes and the respondents' perspectives on the subject area.

Additional verification of categories was achieved by swapping a number of interview transcripts with a fellow student who also used the grounded theory approach. In a feedback session following this exchange, codes were discussed and confirmed.
At the end of this lengthy process, a set of codes was devised that captured on a conceptual level what had been expressed in the interviews.

4.1.6.1 Some initial concepts not confirmed

The extended coding process proved to be an important element of data analysis and showed that some concepts were not as prevalent as previously identified in the initial coding phase. The category 'Legal', which had been identified in earlier coding exercises became redundant and three broad categories remained: mobile phone, privacy and location data. In addition, the researcher had initially presumed that CCTV would be related to individuals' perceptions of privacy and technology. This assumption was based on the relevant literature (see section 2.1.4) and also

potentially on a cultural bias. In the researcher's home country, Germany, the use of CCTV is not as wide-spread as in the UK, which is known to have the most CCTV cameras in Europe (see section 2.1.5). However, in contrast to the researcher's initial expectations, the respondents did generally not identify CCTV as interrelated to privacy. Instead, many of the interviewees talked about the benefits of it and described a trade-off between privacy and security in relation to CCTV. Later on this would become relevant regarding the development of the Core category 'Balancing' (4.2.4 Development of Core category 'Balancing').

Every interview conducted during this study was transcribed and coded immediately after it took place, which was an essential element of the grounded theory methodology. This routine helped to bring up early findings which could then shape subsequent interviews and therefore guide the data collection from early on. For example, initial results from interviews and survey showed that participants did not perceive topics such as CCTV and loyalty shop cards as related to privacy as strongly as anticipated by the researcher.
Consequently, the second interview phase used the existing findings and codes as a guidance and followed Charmaz' (2006) advice to sample along the categories in order to develop them. In other words, the researcher selected individuals as relevant to the initial codes and categories. The focus of subsequent interviews moved away from CCTV and loyalty cards and towards mobile phone use, privacy and location data. This meant for example to interview mobile phone users who perceived their phone as an important part of their lives and others who either did not have a phone or did not use it on a frequent basis. In addition, people older than those taking part in the pilot study were approached in subsequent interview phases. The interview conversation was structured around user's relationships to their mobile phones, individual's awareness and opinions of location data and definitions of privacy.

The on-going interview analysis also influenced the interview questions. Questions regarding loyalty cards were omitted in the second interview phase ,and questions were more open-ended so that participants could talk more about what was important to them. Prompts were increasingly used to learn about respondents' meanings of words instead of making assumptions. Appendix D shows the set of interview questions used for the second phase of interviews, Appendix E shows questions for the third interview phase.

4.2 Development of categories based on interview data

The second phase of interviewing and coding helped to develop the initial codes further. This focused coding phase was more directed and selective than the initial phase of open coding. The focused codes were not meticulously assigned to every single line of interview transcript but made use of some initial concepts to focus on specific issues. These concepts were, for example, the respondents' relationship with their phones and the status of the mobile phone in a person's life.

These focused codes have particularly guided the development of categories. In the following sections the development of the Core category 'Balancing' is described in detail to demonstrate the process of developing categories from codes. The development of categories was facilitated by two intertwined processes; for one part the iterative process of coding, which used different methods to help verify the codes, and for the other part reflecting on the codes, facilitated by memos, to establish links between codes and tentative categories. In order to give an insight into this process and to illustrate how the researcher has arrived from the interview transcripts at the final categories, codes, categories and memos will be presented and explained in the following sections.

4.2.1 Summarising the focused codes

Table 4.2, below, shows a list of codes that were devised based on the multi-staged coding process as described in the previous section and in the methodology chapter (see section 3.3.5 Interview coding). More detailed descriptions and comments to each of the focused codes can found in Appendix K - Quotes for codes.

Table 4.2: List of focused codes

A_Phone usage	**B_Location**	**C_Privacy**	**E_"State", "they"**	**F_Other**
A.1 [Phone ownership] a) [duration] b) [handset] c) [spending] d) [Contract type] A.2 [Features of phone being used] a) Type of feature b) Frequency of use A.3 [Attitude towards mobile phone technology] [Use phone to coordinate social interactions] A.4 [Use phone/ ringtone settings according to situation / location] A.5 [Being reachable (via phone)] A.6 [Being able to contact others] A.7 [take phone with me] A.8 [phone switched on] A.9 [Being dependent on phone]	B.1 [location data] a) [generation] b) [storage] c) [ownership] d) [access] e) [dissemination] f) [regulation] g) [use] h) [reliability] / technical details i) [accuracy] j) [history – realtime] k) [existence of loc data] B.2 [Having knowledge about a person's location] B.3 [Parents tracking children] B.4 [Feeling about one's location]	C.1 [space] C.2 [controlling information] C.3 [liberty (to do things)] C.4 [bodily privacy] C.5 [balancing act] **D_Emotions, "me"** D.1 [trust] D.2 [being/ feeling respected] D.3 [worrying] D.4 [thoughts about future] D.5 [data/information about me] a) access b) financial c) share	E.1 [Law] E.2 [CCTV] E.3 [Attitude towards government] a) Menwith Hill E.4 [Big brother (state)] E.5 [safety-security] E.6 [Crime] a) serious crime E.7 [terrorism] E.8 [ID card]	F.1 [Other people knowing what I am doing] F.2 [Doing s.th. wrong] F.3 [being monitored] F.4 [use of data] a) share data b) my knowledge about it c) consent d) [combining data] F.5 Attitude towards commercial businesses] having knowledge about me a) Marketing b) Selling of personal information c) junk mail d) loyalty cards F.6 [other people] F.7 [being anonymous] F.8 [Other people knowing about aspects of my life] F.9 [reason]

The focused codes listed above are based on codes developed with help of post-it notes (see Appendix I). After adding comments and notes, each interview was re-coded electronically with the NVivo software. By going through the process of coding the interviews on paper, noting the codes on post-it notes and entering those into the computer, the codes and categories were re-fined and reaffirmed. Appendix J provides an overview of the different coding phases.

The final list of codes could be grouped into five themes that were of importance to interviewees in relation to mobile phone location data and privacy (see Table 4.3, below).

Table 4.3: Groups of focused codes and their descriptions

Groups or themes of focused codes	Description of the code
1. Mobile phone use	▪ Phone ownership (details about mobile phone contract, usage, settings and reasons for getting a phone) ▪ Features of phone used (use ring tone settings according to situation) ▪ Awareness of & attitude towards technology, relationship to phone, including feelings (being contactable via phone, being dependent on phone)
2. Location	▪ Location data (awareness of, thoughts about regulation, storage, technical aspects, ownership, access, dissemination) ▪ Implications of knowledge of one's location (feelings/thoughts about one's location, use and misuse of location data: parents & children, workplace
3. Privacy	▪ Participants' definitions, what is it about (space, controlling information, liberty to do things, bodily privacy) ▪ Balancing act
4. Emotions, "me"	▪ Trust, feeling respected, worrying, thoughts about future, information about me: financial, access to information, sharing information
5. State, "they"	▪ CCTV, attitude towards government, Big brother, safety/security, crime, terrorism, ID cards ▪ Other people knowing what I am doing, (not) doing something wrong, being anonymous ▪ Attitude towards commercial businesses (loyalty cards, etc)

Coding interviews constitutes an important link between collecting data and developing theory. Grouping the codes under different headings or themes, together with writing memos has helped to make sense of the respondents' statements. Particularly relevant codes have been explored in further depths, for example by looking at their properties and dimensions. These could then be interlinked and related to other codes to devise more abstract categories. Categories represent the basis for the developing grounded theory, which aims to explain and sometimes predict phenomena based on empirical data (see Methodology chapter section 3.1.1.2).

The following sections illustrate how the focused codes were used to develop the final categories. Memos allow an insight into the analytical process guided by grounded theory methodology. At the end of this lengthy process of coding, memoing and developing categories, a grounded theory was developed explaining individuals' views of privacy in relation to mobile phone location data (see Chapter 5).

4.2.2 Using a situational map to appreciate the wider social context

While conducting and analysing the interviews it became evident that location data and privacy could not be seen in isolation but needed to be placed within the wider political and social context that the respondents were experiencing at the time. In addition, the study aimed at developing a *substantive grounded theory* that interpreted and explained the subject area in a specific setting. In other words to describe individuals' views of privacy in relation to mobile phone location data within the context known to the participants of the study. It was not the aim of this study to make the findings generalisable across the UK or the rest of Europe. This would have been addressed by a more general theory, known as a *formal grounded theory,* which is less specific to a time, group and place but considers a wider range of settings, concerns and problems, taking into account a variety of conditions (for more detail about substantive and formal theories, see Chapter 3 Methodology, section 3.1.3). In order to help recognise the interviewees' micro and macro relationships, which may have shaped their perceptions of mobile phone location data and privacy, a situational map was constructed. Developing the situational map helped to identify the elements in the situation of concern and to examine the relations amongst them. Situational maps can also assist in deciding which GT codes to keep and pursue and which are no longer important (Clarke, 2005).

The starting point for a situational map is the situation of concern, which can be described for this study as follows: Mobile phone location data has to do with privacy as it is data generated by every mobile phone and hence reveals information about the mobile phone user. However, the matter is whether mobile phone users perceive location data as personal data and therefore would like to claim control over it. This also makes it a political issue as mobile phone service providers are required to store the data, which is then accessed by governmental organisations. The situational map, below, lays out the most important human and non-human elements in the situation of concern. Ten categories or areas as suggested by Clarke (2005, p. 90), have been used for reflection and ideas (see Table 4.4, below). A memo was written to keep a log of those ideas (see Memo 1,

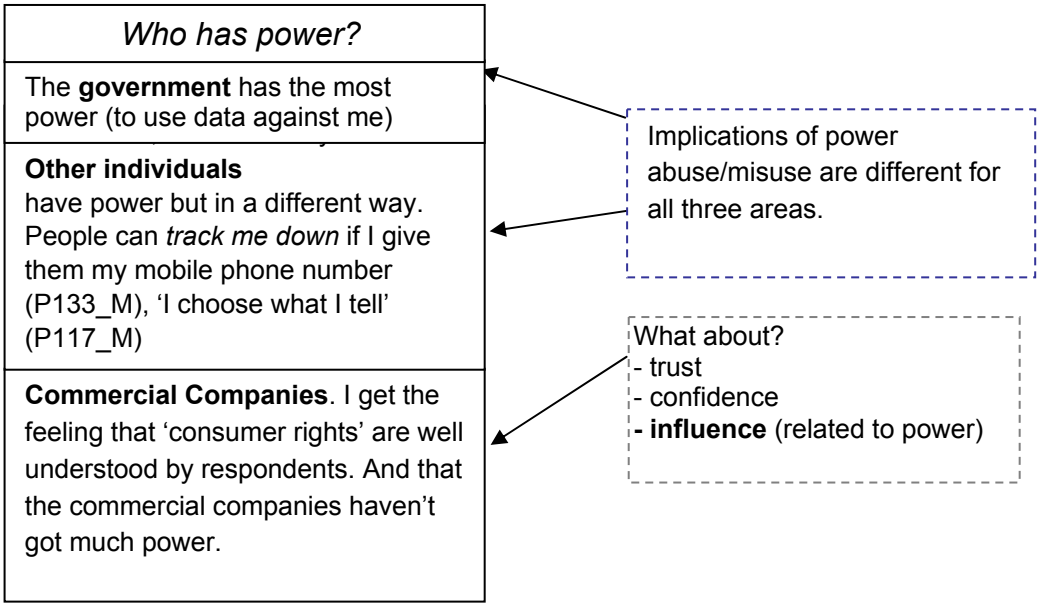
below). When using grounded theory methodology, memos reflect the researcher's thoughts and ideas at the time of data collection and analysis. A discussion of the empirical findings in relation to the literature will therefore be provided in the following Chapter 5.

Table 4.4: Situational Map (after Clarke, 2005)

Individual Human Actors Unorganised private individuals, such as - mobile phone users - non-mobile phone users - criminals - terrorists	**Collective Human actors** <u>Organisations</u> - mobile phone service providers (such as O2, ..) - commercial organisations (retail businesses, marketing) - UK government, EU commission ('legislative') - police ('executive') - emergency services - NGOs (e.g. Privacy International, Statewatch) - terrorist and criminal organisations
Political Elements - political parties - government / parliament {the gov.'s 'task' to provide national security} - NGOs (see also Organisations) - is terrorism a political element? **What *if*** there would a lesser terrorist threat? Would data retention not be an issue then? Would any other uses for the retention of communications data be advocated?	**Economic Elements** 'Condition' of - economy (fairly good) - particular industries - mobile phone - handset - service provider - network infrastructure - internet service providers -> **What *if*** the economy was worse than now, would the situation of data retention be the same? Would this mean- fewer handsets on the market (& mobile phones not as wide spread in society) - data storage costs could be too high to make blanket data retention possible
Temporal elements - 9/11, terrorist attacks in Sept. 2001 in the US - 07/07, London terrorist attacks in July 2005 {I call these 'temporal' because these events have lasted only for a few moments. However, the political and social impacts have lasted much longer.}	**Major issues / debates** In the daily politics - security and 'fight against terrorism' vs. civil liberties and privacy (particularly after London terrorist attacks, July 2005) - ID cards
Non-Human Elements <u>Technologies in general</u> - trend towards digital generation, access and storage of data, - increasing access to broadband internet, ubiquitous electronic communications (email, chat, voice-over-IP) <u>Mobile phone technologies</u> - handsets: mobile phones as versatile lifestyle accessories: music player, organiser, games, .. - mobile phone network infrastructure: 99.9% coverage in UK	**Socio-cultural / symbolic elements** - the British population does not want to have (biometric) ID cards - mobile phones as 'life style accessory', a 'must' for many: OAPs to school kids (safety, connectivity, convenience) - Britain's multicultural society
Spatial Elements - spaces relevant for situation. How accurate is location data? - geographical aspects of terrorism: (Yorkshire), UK, Europe, the world	**Related discourse** - *Normative expectations* "in the name of terrorism, I am happy/expected to sacrifice my privacy." - mass media: terrorism needs fighting with all means

Memo about situational map, taking into account power relationships

Mapping the social conditions that might be experienced by interviewees in daily life has helped me to highlight the position and influence of stakeholders involved with location data, such as NGOs and security services.
The situational map has emphasised the relevance of the phenomenon terrorism, which can be classified as political element. Terrorism has an impact on major issues and debates of Britain as a nation. Currently, there are numerous discussions in the media, revolving around national security, such as ID cards and the introduction of new terrorism laws. Temporal events such as the 07 July 2005 London terrorist bombings have added to the increased media coverage about national security. Particular these temporal events have led to the normative expectation of the government towards the general public to sacrifice some privacy in the name of terrorism; 'there is nothing to fear for citizens if there is nothing to hide'.
And of course the widespread use of electronic communications, predominantly the mobile phone, has a great impact on the situation of concern. All these reasons have turned the long-term retention of communications data (incl. location data) into a widely accepted utensil in the government's tool box for the safeguarding of national security and fight against terrorism.
Related to all these human and non-human elements is the notion of power. Respondents mention a link to power regarding different data collections and seem to perceive a varying degree of power of other actors depending on the area in their life (see graphic below).



Memo 1: Memo about situational map, taking into account power relationships

Participant P136_F provides the following reflection on the retention of mobile phone location data:

> "The fact that like, **it's a way of controlling people**. People's movements. And the fact that like that you are thinking, you are being watched and there is government organisations and like people who have more **power** and they are able to .. kind of .. manipulate your actions or **control you through fear of ..** kind of doing wrong or .. ehm, .. sort of leading towards, leaning in towards more criminal activities or something. So, .." (P136_F).

Memo 1, above, together with P136_F's thoughts (see quote, above) about power relationships have prompted the researcher to further explore the relationship that individuals have with the government and the importance of power.

4.2.3 Category 'Process of monitoring and use of data'

The following issues have been raised by the participants when reflecting on individuals or organisations having access to their personal information and to their mobile phone location data:

- **Who** is tracking
- **Reason** for tracking, why?
- Concern about **what** might happen to collected data (this depends on who is tracking – see interview P117_M), What is data used for (P135_F)
  How is data used (P134_F)
- **Who is** going to have **access** to information (P135_F, P131_F)
- **Consent** of user is needed to pass data onto somebody else (P135_F, P134_F, P131_F)

For the participants of this study it is important to know who uses and has access to their mobile phone location data. Often people stress the point that the act of being monitored or 'observed' does not concern them (e.g. 119_M, 118_F). This particularly became evident in the pilot study, where the participants could have potentially been 'under surveillance' at any time while taking part in the study. P119_M's quote below shows that it seems to be most important to respondents to know the *reason* for being monitored.

> "So, it's not necessarily somebody tracking you, it's more what they do with it. And the **reasons** why they are tracking you is more important than actually being tracked yourself" (P117_M).

> "You'd wonder why. (..) But eh, yeah, unless they'd come up with some reason which I can't think of other than but, some **justifiable reason**. Then fair enough" (119_M).

Respondents believe that depending on *who has got access* to the data will have an effect on the *use of data*. *Who* has got access to my data and how much '*power'* they have got defines the scope for *potential misuse*. This is seen as being far more important than the 'process' of being monitored.
The respondents trail of thoughts can be conceptualised as illustrated below (Figure 4.11, below).

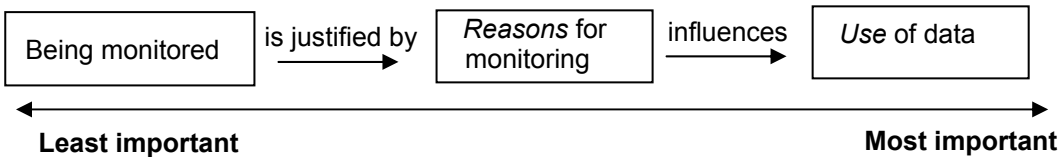


Figure 4.11: Steps of a monitoring process and their importance

The respondents describe the process of being monitored, such as for example by a CCTV camera, as justified by a reason, such as recording images for future crime investigations. This reason for monitoring is perceived to drive or influence the use of the collected data.
For the respondents of this study, the actual act or process of being monitored, particularly having their location data recorded, is the least important step in this chain of processes (Figure 4.11). Of most importance to the respondents is the actual use of data, which relates to Participants' privacy definitions (section 4.2.10). In addition, all three steps of the monitoring process are affected by *who* is monitoring and their position of power in relation to the subject under scrutiny.

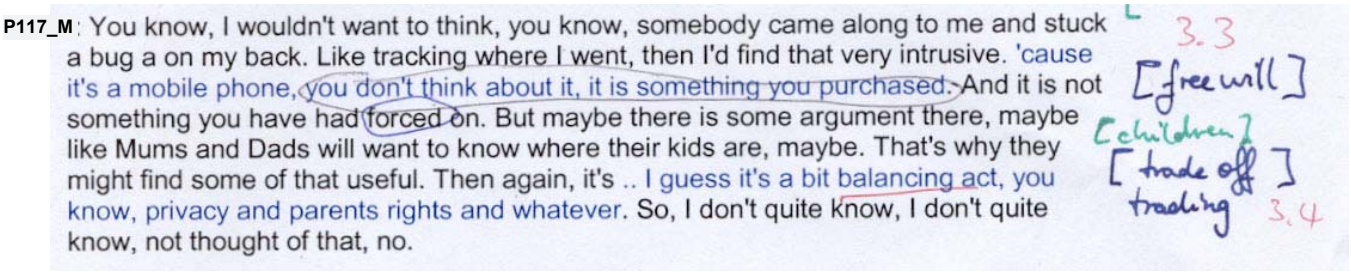
4.2.4 Development of Core category 'Balancing'

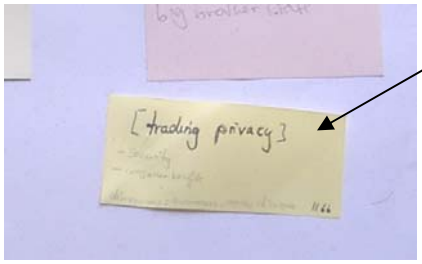
One concept that occurred frequently in the interviewees' accounts was the idea of 'balancing', in the sense of weighing up different needs or requirements, such as privacy with security. 'Balancing' was introduced as a category early on and had been promoted as the core category, also known as the central category (see section 3.1.1.2) because it links up all other themes and findings.
In interviews and survey responses, participants frequently mentioned different areas in life in which privacy plays a role: Firstly, friends, family and other social contacts, secondly, commercial organisations and thirdly, the government. In each of these three areas balancing takes place in relation to privacy. Further detail to this category will be provided in section 4.2.9 Different areas relevant to privacy, below.
The following section outlines the development of the Core category 'Balancing' to provide an example for the coding process as described in the methodology chapter

(see section 3.1.2 Use of GTM for this study).The category balancing was included from early on in the form of an 'In vivo code', which is a code that uses a respondent's words as a code name. In addition, 'Balancing privacy with other needs' was already devised in the first phase of coding the pilot study interviews in NVivo (see Figure 4.8, above).

Post-It Notes - 'trading privacy'

The coding process started off with writing the codes with a pen on the margins of interview transcripts. Following this the majority of codes was jotted down onto post-it notes (see Appendix I). In this coding phase the code 'trading privacy' was noted on a post-it note, based on P_117_M's description of his feelings about using location data for safety purposes (see Figure 4.12, below).





Post-it note reads:

```
[trading privacy]
- security
- consumer benefits

dimensions: awareness, agree,
disagree
```

Figure 4.12: Example on post-it notes for code 'trading privacy'

The codes written on the post-it notes were arranged into groups and different codes related to the concept of balancing or trading were assembled together.

Use of NVivo software - 'Balancing Act'

After coding more interviews and making comparison between them, the NVivo software was used. The code 'Balancing Act' was established within the category privacy, together with several other sub-codes (see Figure 4.13)

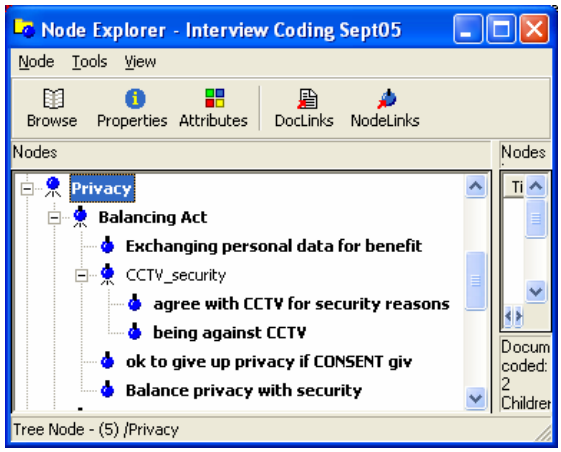


Figure 4.13: Focused codes about Balancing in NVivo

The sub-codes of 'Balancing Act', such as 'Balance privacy with security' and 'Exchanging personal data for benefit' capture the range of situations that this code can be applied to. These different situations correspond to the distinction of different areas of privacy, which later on would become one of the final categories (see section 4.2.9 Different areas relevant to privacy).

Respondents used expressions such as "discourse" (P131_F) or "grey area" (P133_M) to describe the balancing act between privacy and security.

> "Pphh.. (sighs) [pause], Ehm, [pause] **that's a bit of a discourse**. Because I am for the one being, you know civil liberties and they shouldn't be out to track you and do this and do that. But then if it does help track people like that girl from New Year's Eve or terrorism, then I think maybe that's a good thing" (P131_F).

Others described a balancing act between privacy and security regarding CCTV and between getting consumer benefits and releasing personal information with shop loyalty cards, see Figure 4.14, below.

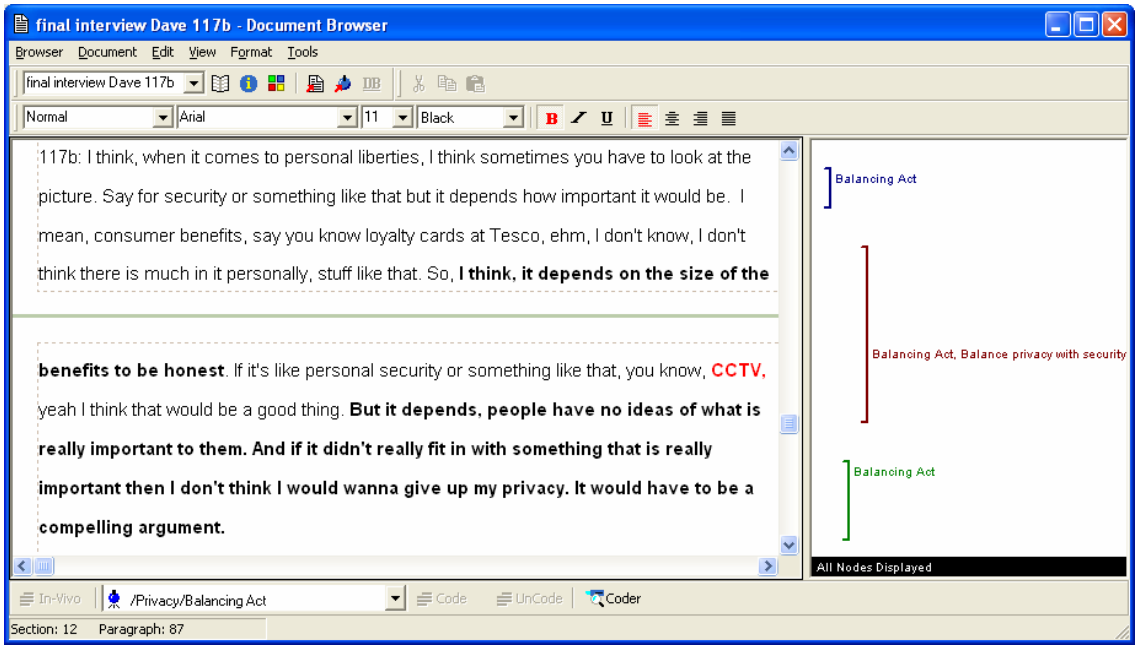


Figure 4.14: Interview excerpt for code 'Balancing Act' in NVivo (P117_M)

Whilst reading and coding the interview transcripts, the researcher has captured her thoughts and ideas about the category balancing act in memos, such as for example the following:

Memo 'Balancing security and privacy'

And then there is the issue of people being okay with the government collecting data on people because it is for safety and security reasons.

People seem to be **in two minds**, they don't seem to be too sure whether it would be useful to store location data or not. On the one hand, if the data was stored, it could be used for crime investigations and emergencies. However, on the other hand, storage of everyone's data would mean interfere with individuals' needs/perceptions of privacy. This is a very complex issue with many "variables". Should the data be stored for everyone or just for some suspects? In other words, which one should be preferred 'data retention' or 'data preservation'? In the latter case, there would be a difficulty if someone would only become a suspect after the crime or terrorism act has occurred. This is where the participants start using terms such as **'discourse',** a **'grey area'**. However, this dilemma could potentially be solved by informing people as soon as they purchase a phone that their communications data might be recorded. All participants would welcome a more open policy regarding data retention that is more information provided by mobile phone service providers and the government. It would be possible to integrate 'checks and safeguards' (P135_F) into the policy scheme. People feel that there should be an independent panel (of judges) to decide in every case (of use of location data or communications data) whether the use of communications data for crime investigations is justified by the circumstances. This is the relevant code to use here: **[code: justify measure of crime]**.

Memo 2: Balancing security and privacy

After establishing some tentative categories, such as 'Balancing act' and different areas of privacy, such as social contacts and the government, potential links between these categories and individuals' attitudes to mobile phones were explored.

4.2.5 Use of mobile phone settings to regulate privacy in the social area

Every interview was initiated by inviting people to talk about their mobile phone and mobile phone use in general. It quickly became apparent that mobile phone use - the participants' own use and that of others - was perceived as related to privacy. Numerous codes regarding mobile phone were devised, as can be seen in Figure 4.15 (right). Some codes related to the use of mobile phones, such as the code 'having the phone switched on' or 'features of phone used'. The interviewees talked about how they used their phones in day-to-day life and the researcher identified that many used their phone to manage or influence how others would get in touch with them. The code 'use of mobile phone to manage social interactions' was applied to sections such as the following, where P117_M describes the different phone setting he uses during a normal day:

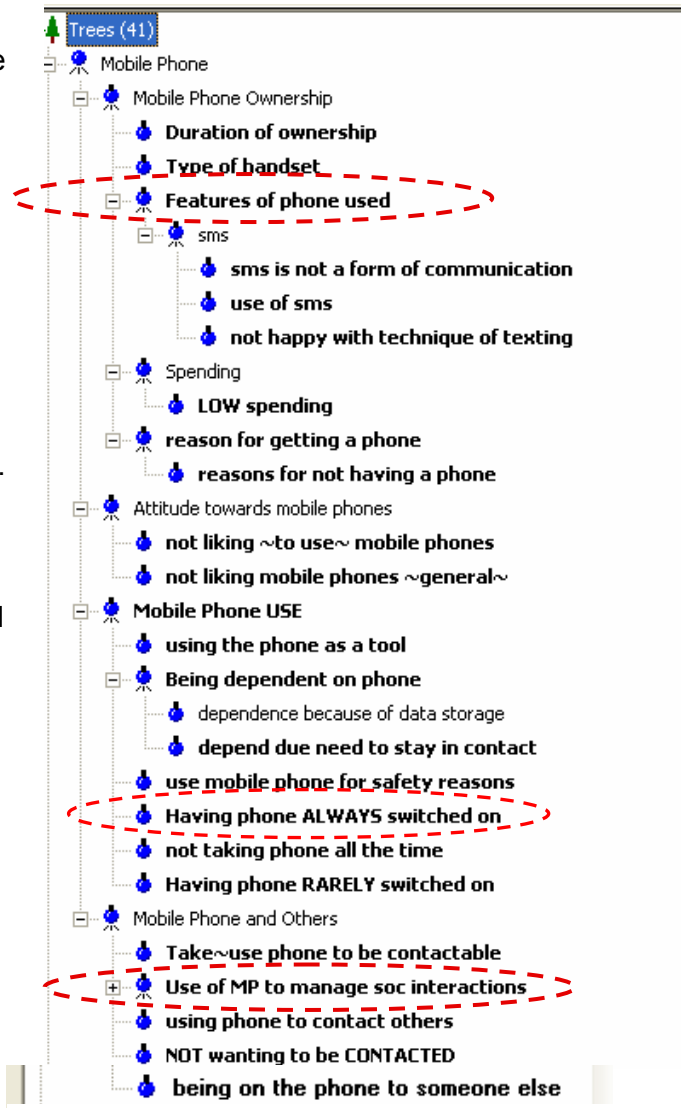


Figure 4.15: Codes relating to mobile phone use

> P117_M: "I generally have it switched on all the time but usually have it on **discreet** for most of the day. This is when I am at work, I don't want to be disturbed and when I am **at home** too knackered to pick it up by large.
>
> A: and you also have it switched on at night?
>
> P117_M: Yeah, I do but I tend to put it on **silent** because eh.. you know people tend to text message and stupid things.

At the same time as talking about mobile phone settings, respondents described particular routines related to their phone usage, such as

> "And then, ehm, it goes on in the **morning**. Because I got a phone at side of bed, you see. And I just look at it, like when I go to my lunch. And go over to me office to have my **lunch** and have a quick look and do any phone calls or

> text messages if I need to. And then mid **afternoon** and **evening** when I get home, before I sit down to watch TV" (P135_F).

To capture this phenomenon of phone use, the category ‘use of mobile phone to manage social interactions’ was developed. This category encapsulated the different codes relating to mobile phone use.

Following Strauss and Corbin’s (1998) advice, properties and dimensions were developed for some of the tentative categories to map out the characteristics of those and to explore their meanings (for detail see section 3.1.1.2). Dimensions can be used to recognise variations of that category and of the final theory. Table 4.5, below, provides an illustration of the properties and dimensions of the category 'Use of phone to regulate social interactions'.

Table 4.5: Category 'Use of phone to regulate social interactions' and its properties and dimensions

Category	*Properties*	*Dimensions*
Use phone to 'regulate' social interactions	- Ring tone settings	ring, vibrate, silent, mute, switched off
	- Features of phone used	voicemail on/off
	- Phone with person	Yes, no, usually rarely

The following memo has helped to reflect on the category ‘use of phone to regulate social interactions’ and its meaning.

4.2.6 Memo 'Using the mobile phone as a tool'

Memo and 'Relational statement' about mobile phone use (after Strauss and Corbin, 1998)

The mobile phone is used as a means of communication, either direct (voice calls) or temporally delayed (text, voicemail). The mobile phone has become part of everyday life, part of family, work and emergency. People develop certain routines when having[1] a phone. Many people do not leave the house without their keys, their wallet and their mobile phone, as the following respondent describes:

> "I think, they've just become part of life now, haven't they? I now, as soon as I get up in the morning and put my clothes on, the **first thing** I do is put my mobile into my pocket" (P137_F).

Strauss and Corbin (1998) advocate the use of so-called relational statements to explore a phenomenon.

1) **When** some people are bored or have some spare time on their hands, such as when travelling (see P119_M), the mobile phone is considered a welcome tool to 'kill time'. It enables to get in contact with others, play games or access the internet via WAP (to access published information).

2) 'Using the mobile phone for non-(direct) communication' (games, WAP, radio; text) is the **action/interaction** to 'kill time'

3) As a **consequence** of 'trying out the functions of a mobile phone', those people are likely to acquire 'a good knowledge about using a mobile phone' and are able to 'use their phone as a tool' (i.e. be in charge of phone, be able to use

Memo 3: Using the mobile phone as a tool

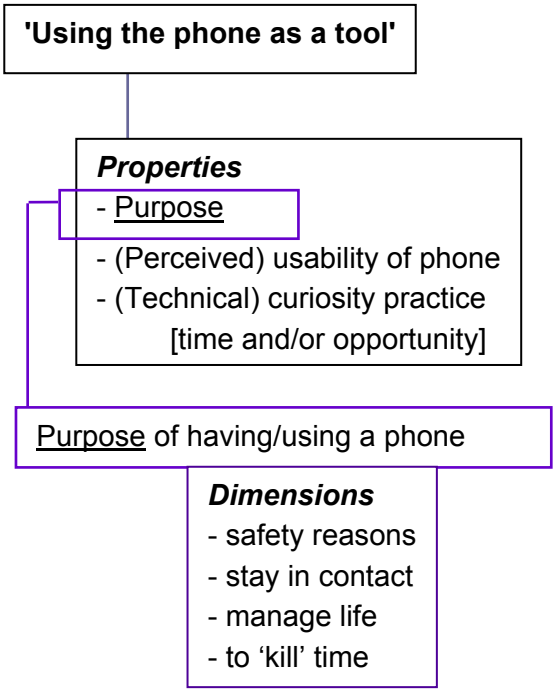


Figure 4.16: Category 'Using phone as a tool' showing properties and dimensions

Figure 4.16 illustrates the category 'using the phone as a tool' and shows its properties and dimensions. A phone is seen as a means of communication but also as a fashion accessories and a handy gadget, such as music player, camera. A phone can be used for various *purposes*, and voice communication is only one of them. Mobile phones can be utilised to make someone available to others and to contact others, to organise or manage one's life from doctor's appointments to

[1] The term *'having'* (a phone) instead of *'using'* is utilised deliberately in this context, as these routines are evident even if the phone is not used for communication.

babysitting. Phones are most frequently carried for safety reasons (car break down, fewer phone boxes around and so on). Phones can be used to 'kill time' with help of functions, such as games, radio, camera, calendar, internet access (WAP). This seems to be more pertinent to the younger generations, who have not got a set work place with constant internet access but spend a lot of time on the move. There are skills to be learned when using a phone and these need time and practice. In addition, perceived usability of the phone plays a role and can encompass attitudes towards writing text messages and the motivation to adapt to small screens.
The traditional landline phone number is for one place, a mobile phone number is for one person. Mobile phones tend to be carried 24 hours per day, everyday by the respondents (see section 4.3.2, below). Hence, the mobile phone is a very personal device and relates mainly to the area of privacy of social contacts and not as much to commercial companies and government.

The method of breaking down a category into its properties and dimensions, as advocated by Strauss and Corbin (1998), proved to be of limited use for the analysis. For some categories it was possible to devise a number of suitable properties. However, the researcher decided that for most of the categories it did not make sense to assign properties and dimensions, as this forced the qualitative data into a rigid framework without adding much value to interpretation of data and analysis. Instead Charmaz' (2006) approach was adopted, which uses the less restrictive way of making comparisons between data (see also section 3.1.1.1).

4.2.7 Different types of mobile phone users

The primary purpose for which a mobile phone tends to be used depends on the *type* of mobile phone user. Even though it has not been the aim of this study to identify different types of mobile phone users, the variations in phone use between the different respondents could not be overlooked when conducting and analysing the interviews. Principally two types of users can be distinguished:

Table 4.6: Two types of phone users

Type of user	Low User	Power User

User characteristics	- low spending
	- older handset model
	- often on pay-as-you-go contract
	- phone mainly for
	  - travel
	  - emergency
	  - sometimes shared with someone else
		- higher spending
		- colour phone, often with camera
		- monthly contract
		- use phone as 'toy' (games, used for non-communications)
		- sometimes the only phone, no landline.

Power users use their phone on a day-to-day basis and tend to be very familiar with the settings of their phone. These users tend to carry their phone at all times and use their phone as a 'tool', for example for storing information, games, to keep in contact with peers. Power users often deliberately use settings to ‘regulate their contactability' (see 4.2.8 Category contactability), for example by switching the phone to voicemail, and or setting the phone on silent or vibration.

> “Yeah, I think, I used to put it on **silent**, like, when I am **at work**, if I am like doing **visits for work**, I had it on silent or sometimes I might **turn it off** then” (P136_F).

Low users tend not to use their phone on a regular basis but mainly for travelling and security or safety related purposes. The mobile phone does not play an important role in the everyday lives of these users. Low users can usually be reached by family and friends by other means of communication than their mobile phone. Many low users tend to view the relationship between phone and contactability as *critical* or *disapprove* of it, as for example P132_M explains "I hate phones, I only got it to run trips. To be contactable”. These users feel annoyed with mobile phones and often purposely do not carry their phone or do not give out their number, as P113_M reveals:

> "Ehm, I was travelling quite a lot I think at the time. So, we got it [the mobile phone] just to be able to call home. Or in case the car broke down. **I don't give my number to anybody** - **ever**. Not even my mother. Like it's kind of a transmitting device, not a receiving device" (P133_M).

Monetary constraints, age, family status (single or with family) have an effect on the use of a phone and hence on the mobile phone user category. However, these influences related to demography were not explored in detail as this was not directly related to privacy and hence not an aim of this study.

4.2.8 Category contactability

A mobile phone can be used to manage or regulate social interactions, as described in previous sections, such as section 4.2.5 (Use of mobile phone settings to regulate privacy in the social area). The traditional communications model 'Sender-Receiver' has been modified to reflect this role of the mobile phone.

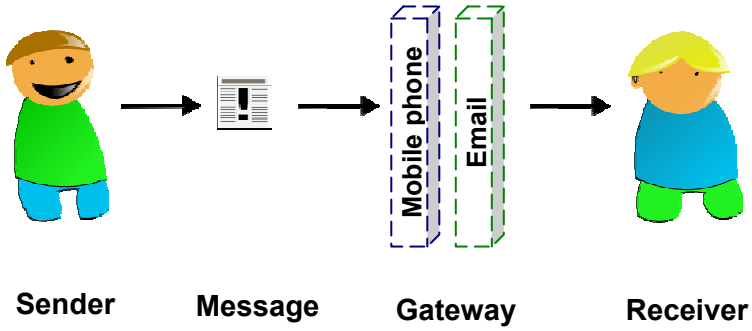


Figure 4.17: Communications model 'sender -> message -> *gateway* -> receiver'

The mobile phone acts as a gateway to a person through which the message is delivered from the sender to the receiver (Figure 4.17, above). This model has inspired the researcher to write the following memo about contactability.

Memo about Contactability

I can ring out to arrange meetings with friends but I can also give out my number and receive phone calls from people. People are reachable through their mobile phone. It is one of several 'gateways' to a person, it gives others access to a person / someone. Other gateways might be other means of getting in contact with a person, such as the landline telephone, email and of course face-to-face contact.

Other people's access to oneself through the mobile phone can be summarised as 'contactability'. The concept of contactability is related to a person's feeling of having privacy. Some people feel that being constantly available to others means a reduction in their liberties and a restriction of their privacy. They do not want to be reachable at all times. Others do not mind. Some people mention that other people talking on the phone impacts on their privacy. Possibly, because the person listening to someone else's conversations is annoyed by this behaviour. This can be summarised by the following graphic:

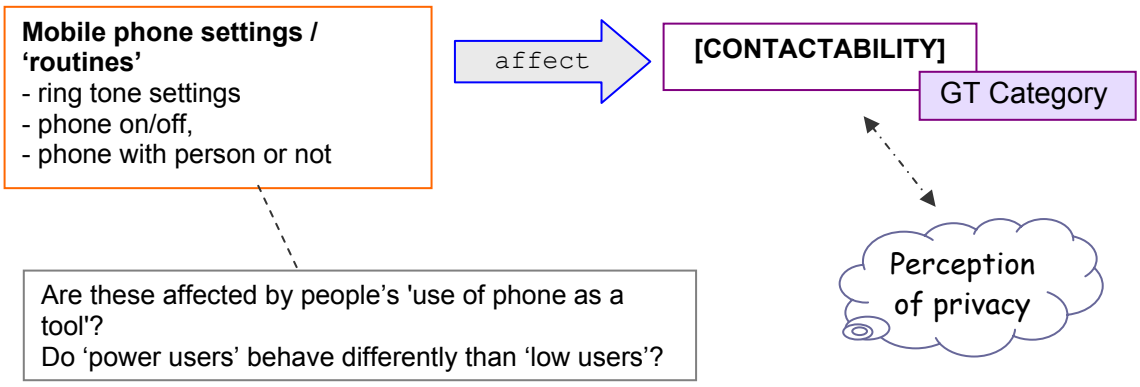


Figure 4.18: Relationship between phone settings, contactability and privacy

Memo 4: Memo about contactability

The mobile phone has got the ability to interrupt on-going conversations and to take over the mobile phone owner's time while he or she is still physically occupied with other social contacts. This is seen by some people as a negative side of mobile phones. For example, respondents perceive it as rude behaviour to be on the phone while being with someone else.

> ".. in a railway carriage and somebody is like yakking on their mobile phone and like that's **invading my privacy**. And also I think if you are out with somebody and then their phone goes, yeah, and they spend all the time **talking to their phone and not to you**. Well, I don't know whether that's privacy but that's kind of .. I think that's wrong anyway, **rude**, whatever" (P133_M).

Phone settings tend to be used by phone users to 'regulate their contactability' (see Figure 4.18, above). Phone settings can consist of ring tone settings, such as ring, vibrate, silent or switched off. For example some phone users, carry their phone at all times and have it on a setting which allows them to be immediately aware when the phone rings. Others only carry their phone sporadically, do not use voice mail and if they have got their phone on them, they put it on silent. This means, that when a phone call arrives, it might potentially go unnoticed because it is only signalled by one short beep. Hence, the settings of a phone have an effect on a person's availability to others, in this context known as 'contactability'. Mobile Phone users develop certain routines regarding carrying their phone and phone settings, such as putting the phone on silent when arriving at work.

Some participants have the feeling that they can be "tracked down" (P133_M) when they have got their phone with them. Others feel that being constantly available to others has an impact on their ‘space’ or in other words their privacy, see P134_F’s comments below:

> "You know one of the reasons why I necessarily won't have my phone turned on is because I don't want people to be able to **contact me all the time**. I don't want .. you know I want to have that .. **space**" (P134_F).

The participants’ use of their mobile phone to regulate how and when others gain access to them supports this study's claim that respondents see privacy predominantly as related to themselves and their own lives. Hence, arguments by the literature and civil liberties organisations (see section 2.2.5) that the routine and long-term retention of communications data is a form of surveillance and can potentially have negative effects on society, do not seem to relate to the view of privacy as voiced by the participants. This discrepancy will be discussed in further detail in Chapter 5 (section 5.3).

4.2.9 Different areas relevant to privacy

Individuals' descriptions of privacy vary depending on the context, as indicated in previous sections. This perception of different areas of privacy became particularly evident when one of the interviewees talked about privacy as being on different 'scales', with each scale impacting on different areas of a person's life:

> "Well, I suppose, it depends what you mean by privacy, really. And like how you define it and .. in what sense you mean. 'cause I think, there is **privacy on different scales**. Like there is like on **smaller scale in your own immediate lifestyle** and sort of **family and friends** and your home.. and your workplace. And then there's like the **wider sense** in terms of, you've got down here CCTV and data tracking [points to my sheet with interview questions] and stuff like that, location data" (P136_F).

P136_F's depiction of privacy summarises other interviewees' descriptions of privacy. Most respondents distinguish the following different areas of their life in connection to privacy (see Figure 4.19):

- Friends and family - social interactions (blue circle)
- Commercial companies - marketing, loyalty cards (red circle)
- Government - CCTV, Data retention (green circle)

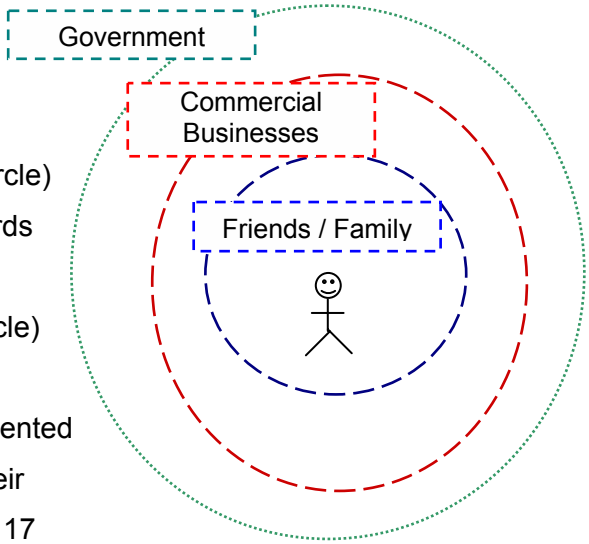


Figure 4.19: Three different areas of privacy

These different scales or areas of privacy were presented to participants in subsequent interviews to obtain their comments (see for example Appendix H, interviews 17 and 18). Following the constructive responses, the initial theoretical framework of perceptions of privacy had been developed and is depicted in Figure 4.19, right.

The smallest scale of privacy includes a person's closest social environment, which can be family, friends and sometimes work colleagues (blue circle). The person knows these people and is known to them. Social interaction takes place and there are common friends and hobbies. Personal habits and preferences are known. The next greater scale (red circle) represents commercial companies, who hold particular data about the person, such as shopping habits collected by loyalty cards. The 'green circle' represents privacy in the widest sense and is related to the government. When talking about privacy in relation to the government interviewees mention the recording of data in form of CCTV images and mobile phone

communications data. An *interaction* between the government circle and citizens only takes place under certain circumstances, for example when a law is broken, in case of emergency or in relation to terrorist attacks.
Initially, another circle had been included in this model which represented 'the public' and was wider than the commercial circle. The public includes strangers; people who are unknown to the person and the person feels ‘anonymous’ within the public. However, this has been dropped after re-reading interview transcripts, as it did not seem to be significant enough to the respondents.

4.2.9.1 Privacy relating to friends and family and its relationship to the Category Contactability

In relation to friends and family, interviewees primarily mentioned the concept of liberty. Privacy is mainly about "being able to keep things to yourself" (P119_M) and the term 'private person' has been used to describe someone "who doesn't like to share that much […] who is quite selective about who they want to share.. their life with. Personal things to do with themselves." (P134_F) (see also section 4.2.10 Participants’ privacy definitions)

In the context of the privacy area of friends and family, mobile phone settings play an important role in regulating and determining how other social contacts can get in contact with the mobile phone user. Hence, the mobile phone can be understood as to regulate a mobile phone user's privacy. The metaphor of the mobile phone being a gateway to a person is suitable in this context, as explained in the previous section 4.2.8 (Category contactability).

The following quote shows P117_M’s approach of gaining over control information about his personal life. In order to not share it with others in his social circle, he is very much aware what he tells whom.

> "I think, privacy basically means ehm .. getting away with doing what I want to do without other people finding out. That is pretty much my answer.
> I am a very **private person**, you see. I don't like to tell people what I am doing. I think that, I feel that, if people know what I am doing, then they can tell other people what I am doing, whereas if it's just me and I know and it's private, then I can **keep it all under control** in that sense" (P117_M).

Whether they wanted to share the data or not, most frequently interviewees would want to know the *motivation* for someone else wanting to have access to their data.

> “Mmh, no. other than more concerned about the reasons for doing it rather than actually being tracked.” (119_M)

4.2.9.2 Privacy in relation to commercial companies

The commercial circle of privacy relates for the most part to individuals' personal data. Some interviewees mention that they do not mind giving access to data about their shopping habits to certain companies, as long as it is ensured that it will stay within those companies; "I don't mind giving them my details as long as they hold on to them, like Tesco" (P131_F). However, some interviewees do not like to share any information about themselves with commercial companies at all, "I hate them, I hate them. Because they take your information as well and use it to make more money for themselves. And con you into buying more stuff you don't want." (P132_M). Whereas others, such as P137_F, did not seem to be aware of these data collections "I didn't realise, they collected the data about what you buy, do they?".

Many respondents describe a trade-off between giving their personal information to commercial companies, for example via loyalty cards, and getting benefits from the company in form of 'points' or price reductions.

> "Well, **I use them**. but then again, ehm .. , **they are using me** for information. So, I don't see anything wrong with me using them, so I get loads out of the points" (P135_F).

Interviewees generally would not want commercial companies to have access to their mobile phone location data.

> "That they can track where you live, how much you time you are using on the phone. Who you are phoning from, who long it is, bla,bla (…) You are just going to be **bombarded with all sorts of stuff**" (P131_F).

> "I think, if the information is important, like I said before, for police or whatever, that's fair enough. I am happy they would be able to use it. **But not just for commercial purposes, no**" (P137_F).

This area of privacy related to commercial companies has been identified as the least important one for this study. Firstly, it is not directly related to mobile phone use and mobile phone location data. Secondly, most people seem to be aware of their rights as consumers in terms of data collection. Either they agree to have their data collected (such as P116_F, P119_M, P117_M) or they do not (such as P133_M, P132_M). Respondents frequently complain about junk mail and have developed strategies to avoid unwanted marketing messages and advertisement. The trade-off between exchanging personal information for benefits from

commercial companies is an element of the Core category 'Balancing' (see section 4.2.11, below).

4.2.9.3 Privacy in association with the government and regarding data retention

Awareness of location data mostly comes from the media. Respondents have predominantly heard about mobile phone location data in relation to emergencies, crime and terrorism, as for example a female respondent describes:

> P134_F: "Ehm, yes because of this one program I heard on the radio. (..) it was.. a programme about ehm how new technology is being used by the police to track people ehm, who have **committed a crime**. And find them.
>
> A: yeah, find them afterwards
>
> P134_F: "There was a little bit about that and there was a lot more about retrieving data from the phone. And how that was being used by the **police**."

In this context P117_M fears that "no one is gonna have any privacy", when considering the prospect of having mobile phone location data connected to other governmental databases, such as the DVLA driving license database.

Other respondents make a distinction between the government and other organisations that have an interest in an individual's personal data:

> "... I think, ehm, the government having access is different than like say other organisations having access to privacy like companies and other people. The **government is a bit different**." (P133_M)

Interviewee's responses and thoughts regarding the access to mobile phone communications data by governmental bodies can be grouped into three broad categories, as shown in Figure 4.20, below.

Responses to data retention relating to the government

1) Indignation

a) "I don't think it's right" (to track everyone)
b) Desire to feel respected
c) Wanting to be informed about data collection
d) The government has got an agenda, it wants to control people (terrorism is used as a "moral lever")

2) Resignation

- "That's how it is", "they do what they want"

3) Justification or rationalisation of data retention through terrorism

- Respondents described a 'balancing act' between privacy and security

Figure 4.20: Sub-category: Individuals' responses to data retention

Individuals' responses regarding the access of the government to mobile phone location data can be grouped into three predominant responses: indignation, resignation and justification or rationalisation of data retention through terrorism. Often more than one opinion has been expressed by one respondent during the course of an interview. For example, some respondents express indignation when first talking about the collection of mobile phone data. And later in the interview, they agree with the need for the government to take measures against terrorism and crime. The following sections explicate each of the three responses to data retention, illustrated by relevant quotes.

Response 1) Indignation

Some participants had heard about data retention for the first time by taking part in this study. Hence, feelings of indignation seem an understandable and natural reaction to this new information. Indignation was commonly expressed in the following four different ways:

a) Government should not have the right to track me

Some respondents frequently use the expression 'right', such as the female respondents below:

> "God! I don't think, they've got the **right to hold it** and use it for certain things. I just think, you know, privacy. Why should the police know whether I phone from that mobile and then move across the country" (P131_F).

> "But I don't think it gives the government a **right to track** every single person in the country" and every single minute everyday" (P134_F).

In this context, some people mention Menwith Hill, the American military base in North Yorkshire, which listens for keywords in citizens' telecommunications, and utter strong feelings of indignation (such as P131_F, see quote above).
Others were rather concerned about commercial organisations accessing their data and did not mind the government accessing it (P118_F).

b) Desire to be respected

In the interviews, individuals reflected on the access to location data and its implications and described privacy as related to *respect*. Individuals want to be respected in their immediate social environment (e.g. P119_M and P135_F). However, some expressed the feeling that they did not feel respected by a government that collects data about them without their knowledge, such as this respondent explains:

> "Especially as people, ehm, like your privacy, and your private life is like really sacred to people. So, when that's like affronted [affront = **disrespect**, insult] and when you realise that other people have access to your movements and your location. And you weren't aware of that. ehm, I think, that can cause like clashes,.." (P136_F).

c) Wanting to be informed about data collections

Respondents suggested that customers should be informed about data retention when purchasing a mobile phone. This is not the case as a survey of mobile phone shops in Leeds has shown (see section 5.1.2.1).
One participant mentioned Kafka, who in his book 'The Trial' describes Joseph K. being arrested without trial and without doing anything wrong [2].

> "You know, with the kind of the terror legislation, they tried to get through recently, it is all becoming a bit, kind of **Kafkarish**, I think" (P134_F).

Another respondent describes the stark discrepancy between being and not being informed about data collection:

[2] **"**Someone must have traduced Joseph K., for without having done anything wrong he was arrested one fine morning." [*The Trial* (1925) ch. 1]
http://www.oxfordreference.com/views/ENTRY.html?entry=t91.e1366&srn=2&ssid=536538022#FIRSTHIT

> "Ehm, I think people have a right to know, what the government are monitoring and .. why [raises tone of voice]. I think, it makes everything a lot clearer and it's more **honest**, there is no **deception**. It's fairer, ehm, everyone has access to the same kind of information. Do you know, it's when there is **deceit** and when there is like .. other people are **hiding**. Or like, it seems like things are being concealed. I think, that's when you get more **confrontation** about … stuff. If that makes sense? (…) if it's **concealed**, then you think, why. *Why* haven't I been informed. You know, is there a **different agenda**, ehm. They are **hiding** something, as well" (P136_F).

P136_F's passionate statement about the need of being informed about retention of citizen's personal data has prompted the researcher to write the following memo (Memo 5), below.

Memo - Indignation about not being informed

P136_F's interpretation of the situation of data retention is summarised in the table below. The left hand column depicts the ideal situation for her: All citizens are notified that communications data is retained and accessed for particular reasons by the government. The right-hand column shows the opposite scenario in which citizens are not informed about the on-going data collection. This raises questions about the motivation for not explicitly disclosing that every mobile phone user's data is collated. The respondent P136_F perceives that the current situation in the UK matches the latter scenario and this makes her react with anger and indignation.

Being informed	Not being informed about data retention
a lot clearer	deceit
more honest	hiding
no deception	concealed
Fairer	different agenda
everyone has access to the same kind of information	*Resulting in* - confrontation, - clashes, - problems

Memo 5: Indignation about not being informed about communications data retention

d) A hidden agenda

Some individuals perceive terrorism as a moral lever that is used by the government to justify anti-terrorism but also crime fighting measures. Interviewees talk of the "fear factor" (P131_F) or the "big moral panic thing" (P134_F). People do not explicitly say that they do not trust the government but they seem to suspect a "different agenda". Some suspect that the government wants to control and "keep an eye" on people (P136_F).

Respondents describe different levels of crime which require different measures. The police and government's measures in tackling crime should be justified depending on the seriousness of the crime (see quotes P131_F and 136_F). An independent panel is suggested to provide impartial oversight for the use of mobile phone data to ensure that policing powers can not be misused for petty crimes but only for serious offences. The responded P135_F took a look back in history and warned that oversight over a government's actions is necessary to secure democracy (see Appendix H, transcript 13).

Response 2) Resignation

Often individuals' statements regarding data retention carry an element of resignation. American military bases Menwith Hill and Filing Dales are mentioned in this context:

> "And same like with the mobile phone like I know that the government has **computer programs that listen in for keywords**. Yea, and **that's just how it is**" (P133_M).
>
> "It doesn't help being up by Filing Dales with the Americans; they are sneaky gits" (P135_F).

Some showed little surprise about the storage of mobile phone data, even though they stated that they had been unaware of this practice before the interview, such as for example P133_M (see Appendix H - Interview transcripts).

Response 3) Achieving a balance between privacy and security

In addition to the notions of indignation and resignation, most participants voice the opinion that they agree with the government collecting mobile phone users' communications data for safety and security reasons. Others struggle to come to a straightforward conclusion:

> "So, it's a difficult one. I am sure there are **arguments for** things that they could do with the data but I think there's so **many arguments they could do bad thing**s or stupid things with it. I would be more concerned about them doing stupid things. ... Don't know. I can see the arguments for tracking. **If it's like society gains something from it, *maybe***. So, if it's like criminals, you could track them" (117_M).

> "Pphh.. (sighs) [pause], Ehm, [pause] that's a bit of a **discourse**. Because I am for the one being, you know **civil liberties** and they shouldn't be out to track you and do this and do that. But then **if it does help track people** like that girl from New Year's Eve or terrorism, then I think maybe that's a good thing" (P131_F).

4.2.10 Participants' privacy definitions

The following two definitions of privacy have been prevalent in the interviewees' accounts: on the one hand, privacy being about personal data and control over this data and on the other hand privacy being related to having the freedom to do what one wants to do.

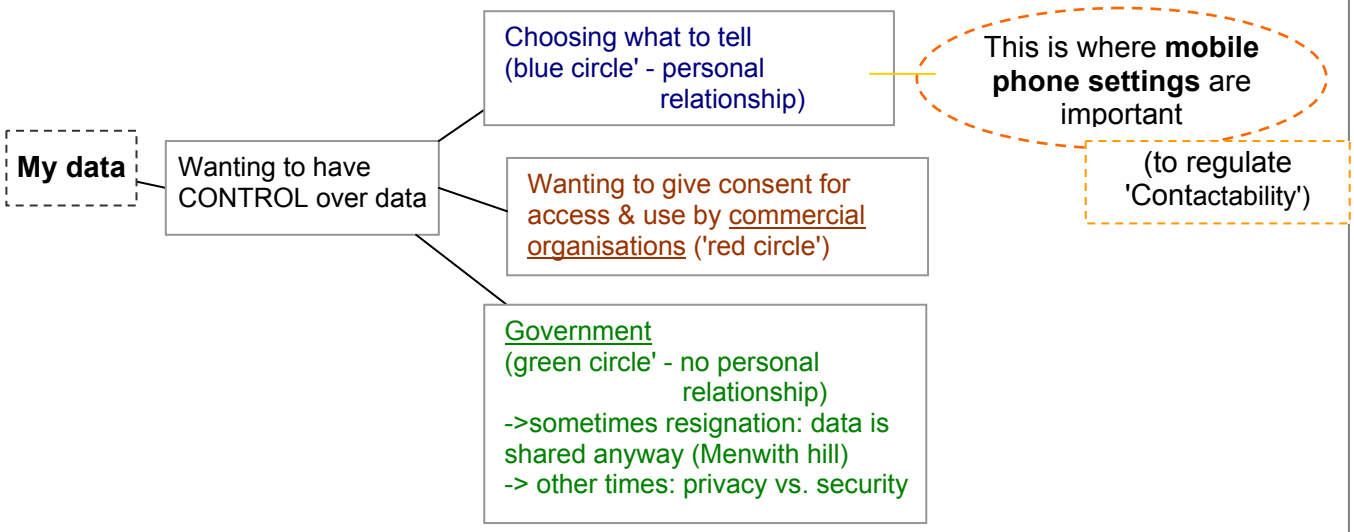
4.2.10.1 Privacy is about my data and having control over it

Participants primarily see privacy as being related to data or information about themselves. They mention for example personal data, such as financial and health information, views and opinions (see transcripts P131_F, P132_M, P138_M, Appendix H). Furthermore, respondents talked about the disclosure of this personal data to individuals or organisations and often stressed their desire to retain control over this data which can be summarised by P117_M's comments:

> "I don't like to **tell people what I am doing**. I think that, I feel that, if people know what I am doing, then they can tell other people what I am doing, whereas if it's just me and I know and it's private, then I can keep it all under control in that sense […]. So, I think basically privacy to me … does equal **control**" (P117_M).

As illustrated in previous memos, respondents describe different fields in life in which their data should be kept private, or in other words not accessed by others without their consent (see Memo 1, section 4.2.2).
This control over data is relevant in all three areas of privacy, as illustrated in the visual memo, below. The importance of personal data to privacy has also been discussed in section 4.2.9 Different areas relevant to privacy, below.

Control over personal data - a visual Memo



Respondents describe the desire to retain control over their personal data. This relates to the previous memo about 'power relationships' (Memo 1) and the Category 'Process of monitoring and use of data' (section 4.2.3). The potential of what can be done with the personal data depends on who has collected the data and who has access to it. For example, respondents distinguish three areas relevant to privacy (see 4.2.9 Different areas relevant to privacy) and in each of these areas a Balancing Act takes place (see GT Core Category, section 4.2.11).

Memo 6: Control over personal data - a visual memo

4.2.10.2 Privacy is about liberty and freedom of doing what I want

In addition to relating privacy to data, interviewees often talk about liberty when probed about the meaning of privacy.

> "having freedom to do things that I want to do, that I **don't have to tick any boxes** to be able to do. And things, so. Individuals freedom, rights, yeah. [Laughs] […]
> I think, privacy basically means ehm .. **getting away with doing what I want** to do without other people finding out." (P116_F)

And as P134_F puts it succinctly,

> "Yeah.. I suppose, privacy can be tied up with being anonymous to some extent. And being able to be anonymous if you want to be; On some level. I think this is some kind of **freedom** in that, on a personal level" (P134_F).

Privacy relates to a 'barrier' between "*me*" and "*them*" or "other people", in relation to social interactions. Respondents appreciate the freedom of "not having to tell other people what I am doing" (P133_M). To 'share one's life with others' means to lower that imaginable barrier and to share some personal information but also feelings and opinions.

4.2.10.3 Privacy is about space

Respondents acknowledge that everyone should be entitled to live their life as they wish, as long as it does not harm others. This relates to the notion of space, which is frequently mentioned by participants in interviews and in the survey. Some explicitly point out a distinction between physical space and mental space, as P134_F explains,

> "and then you could talk about .. private sphere, and **privacy in the home** and things to do with that. And the idea of **private and public spaces**. Ehm..
>
> *A: so, like the home as a private space?*
>
> P134_F: or has been constructed as a private space which has impacted on the way in which it is treated in the law and .. I think, it's about **space**, as well. Ehm, .. but also about the person? And who they are. And how they **feel** about things" (P134_F).

Hence, the use of the term 'space' can be interpreted as follows:

a) When talking about their home, where they can ‘do and be what they want’. (see interview transcripts 119_M, 118_F, P132_M, Appendix H):

> “ (..) you can be private in your house. If you have net curtains up and people can’t see in. but if you don’t, people can see in so it’s not private” (P132_M).

b) The term space is used as a metaphor for mental space, having the freedom to d and to think what one wants (see interviews P135_F, 116_F, P134_F)

4.2.11 Core category 'Balancing'

In each of these three areas of privacy (see section 4.2.9) balancing takes place in relation to privacy. This is illustrated in Table 4.7, below, which summarises the relationship between the area of privacy (first column), Core category 'Balancing' (third column) and mobile phone use (last column). In all three areas of privacy a "technique" of balancing is used to maintain one's privacy.

Regarding *friends and family*, respondents wanted to retain control over their personal information because disclosure could have an impact on their immediate social environment; and privacy infringements in this area are particularly feared of. Concerning *commercial companies*, respondents frequently mentioned a trade-off between receiving benefits in form of points and revealing personal information. As with regards to the *government*, individuals describe a balancing act between personal privacy and national security or protection by the government. In each of these three areas, the mobile phone plays a role regarding this balancing act.

Table 4.7: Relationship between area of privacy and the Core category 'Balancing'

Area of privacy	Description	Relevance for Core category 'Balancing'	Impact of phone on area of privacy
Blue circle - friends and family	Immediate social environment, 'everyday life' and social contacts, such as friends and family.	***Control* over information** (see interviews P117_M, P135_F)	Phone settings to regulate 'Contactability'
Red circle - commercial companies	Commercial companies, such as Boots or Tesco, who hold some data about a customer if she or he uses a loyalty card.	**Benefits vs. sharing data** (see interviews P135_F, who is aware of this 'trade-off', or P132_M and P133_M who are strongly against it)	Phone for receiving junkmail, marketing messages.
Green circle - the government	Interaction with this area takes place only under certain circumstances. For example, when a law is broken, in case of emergency, such as terrorist attacks.	**Privacy and liberty vs. security** (also described as a "discourse" by P131_F or a "grey area" by P133_M)	Location data stored and used for terrorism and crime detection.

Respondents use their mobile phone settings to regulate social interactions in their closest proximity with friends and family. Different types of mobile phone users use different strategies for this. Power users are skilled in utilising the settings of their mobile phone to regulate how reachable they are to other people. Low users use their phone infrequently, the reason partly being that they see constant availability to others as limiting their freedom and their privacy (see section 4.2.8 for more detail).

The mobile phone does not play an important role in the area of privacy relating to commercial companies. The phone could potentially be used to deliver (often unwanted) marketing messages. The privacy related area that is furthest away from participants' day-to-day life concerns the *government*. Recent terrorism threats have prompted the 'normative expectation' to give up some civil liberties, including privacy, to support the government's fight against terrorism. The retention of mobile phone communications data can be seen as concerning individual's data privacy. Respondents explicitly mention this trade-off between privacy and security, and many believe that it is beneficial that communications data can be accessed by police and intelligence services. Others do not agree and show feelings of indignation and resignation. However, these sentiments do not occur in isolation from each other but can constitute phases through which a respondent goes in the space of an interview. The GT Category 'Balancing' represents a major theme of the research and links the different categories that have been established from the interview data. For this reasons the category 'Balancing' has been selected as the core category.
In Chapter 5 - Analysis, these final categories will be contrasted to survey findings and the literature.

4.2.12 A synopsis of the five final grounded theory categories

Grounded theory methodology has guided the data collection as has been illustrated in the previous sections that have discussed the interview findings. In order to demonstrate how the final grounded theory categories were developed, interview codes and memos were presented. The focused codes have guided the development of the categories, while Adele Clarke's situational map has helped to identify the importance of the government in relation to perceptions of data retention. The Category 'Process of monitoring and use of data' encapsulates the steps that respondents identified regarding the process of being monitored and having their personal data collected. In the interviews participants described different areas in their lives in which privacy was important to them, and these have been grouped into the grounded theory Category A - Areas of privacy (section 4.2.9). The privacy definitions that were recurrently referred to by respondents are represented by the grounded theory Category B (see section 4.2.10). The participants' descriptions of privacy were closely related to those commonly discussed in the literature and this will be further explored in the following Chapter 5. The Core category 'Balancing' is linked to and significant for all three areas of privacy that have been identified in the respondents' statements: social contacts, commercial companies and government (see section 4.2.9).

Individuals tend to develop particular routines in using their mobile phone. Often the mobile phone becomes an important tool to manage peoples' lives, particularly for those who fall into the category 'power user' (see section 4.2.7). 'Low users' tend not to perceive significant benefits from carrying a phone every day and every hour. Individuals belonging to this group of mobile phone users feel that the mobile phone truncates their privacy, their space, their liberty by making them always available to everyone who knows their phone number. This highlights that the mobile phone can be used to manage one's 'contactability', in other words one's availability to others (see section 4.2.8). This phenomenon particularly relates to the area of social contacts.

The following table (Table 4.8, below) provides a further summary of the GT Categories developed from the interview data. The table lists all categories and highlights how the focused codes have shaped the developed of each category. In addition, the relevant sections and memos that provide details about each category

are listed. The categories have been labelled with the letters A to E, so that they are easier to refer to in the following chapters.

Table 4.8: List of categories and their relationship to codes

Category	Related theme of focused codes	Development illustrated in section or memo
Category A: Areas of privacy Privacy relating to friends and family - Privacy in relation to commercial companies - Privacy in association with the government	- Privacy, - Emotions, "me", - State, "they"	- Memo 1: Memo about situational map, taking into account power relationships - see 4.2.9 Different areas relevant to privacy -Memo 5: Indignation about not being informed about communications data retention
Category B: Privacy definitions - Privacy is about my data and having control over it - Privacy is about liberty and freedom of doing what I want - Privacy is about space	- Privacy	- 4.2.10 Participants' privacy definitions - Memo 6 : Control over data
Category C: Contactability - use of mobile phone to regulate privacy	- Mobile phone use	4.2.8 Category contactability -Memo 4: Memo about contactability
Category D: Process of monitoring and use of data	- Location	- Memo 1: Memo about situational map, taking into account power relationships - 4.2.3 Category 'Process of monitoring and use of data'
Category E: Core category 'Balancing'	Links to all categories	- 4.2.4 Development of Core category 'Balancing' -Memo 2: Balancing security and privacy - **Error! Reference source not found. Error! Reference source not found.**

The five final categories will be revisited in the next chapter, Chapter 5 - Analysis of Findings, and related to findings from pilot study, survey and relevant literature.
The following section provides a descriptive summary of data obtained by the survey.

4.3 Presentation of survey findings

This section presents the findings from the questionnaire, which has helped to further explore issues raised in the initial interviews (see Appendix L for a copy of the questionnaire). The results will be presented following the structure of the questionnaire, with a summary at the end of this section. The questionnaire was circulated as a paper-based version and over the internet (for details regarding sampling, see section 3.4.1). The results should be taken as indicative and not completely representative as the survey is based on a volunteer sample. The figures indicate a general trend and give an idea of individuals' responses on a greater scale than it would have been possible with interviews.

4.3.1 Three distinct phases of questionnaire distribution due to terrorist attacks

Data collections for research projects do not occur detached from real-world events. The London terrorist attacks in July 2005 occurred while the paper-based questionnaire was being distributed. Because these attacks could have potentially had an influence on individuals' perceptions, it was recorded which questionnaires were filled in before and which ones after the attacks. In addition and taking into account the potential implications of different distribution media, the survey data collection was broken down into three distinct phases: firstly, the paper-based questionnaires distributed before the attacks, secondly those distributed afterwards and thirdly those distributed via the internet. The latter ones were all published after the terrorist attacks (see Table 4.9).

Table 4.9: Three questionnaire distribution phases

Phase of data collection	**Distribution**
Paper-based questionnaire, distributed before 07/07 attacks distributed 16 April 2005 to 06 July 2005	N=248
Paper-based questionnaire, distributed after 07/07 attacks distributed September 2005 to February 2006	N=121
Online survey, distributed after 07/07 attacks distributed 10 August 2005 to January 2006	N=108
Total number of questionnaires distributed	N=477

A comparison between the three phases of questionnaire distribution showed differences only regarding a small number of questions and for this reason the responses of all three data sets were pooled together. Differences between data sets are indicated in the following sections where relevant. The main differences between data sets relate to mobile phone handsets and contracts (section 4.3.2.3), awareness of location data (section 4.3.4) and use of location data for terror prevention (section0). Details are provided in the following sections and complete questionnaire results for each data collection phase are displayed in Appendix M.

4.3.2 Survey section A: Your Mobile Phone

4.3.2.1 Demographics

Out of 477 respondents taking part in the survey 42.6% were female, 56% male and 1.5% did not reveal their gender. The majority of respondents fell into the 25 to 34 age group (31.3%) and into the 35 to 44 year age range (24.6%). Most of the respondents stated as occupation ‘professional’ (29.7%), 'office staff or clerical' (20.6%) or 'student' (16.1%). The likely reason for the predominance of these age groups and professions was that the questionnaire was primarily handed out at the researcher’s place of work (the university) or at friends’ places of work (mainly office environment).

4.3.2.2 Mobile phone use

The majority of all respondents (91.4%) owned a mobile phone, only 7.1% did not own a mobile phone and 1.5% shared a phone with someone else. The majority of all phone users had pay-as-you-go contracts (55.7%), compared to 43.6% of users with monthly contracts. Most users (50.5%) had owned their phone for four to six years. These figures are comparable to national statistics. Ofcom, the independent regulator and competition authority for the UK communications, provides an estimate of around 66.1% of mobile phone pre-paid contracts compared to 33.9% of monthly contract subscribers for the year 2005 (Ofcom, 2006).

55.9% of mobile phone users indicated that they typically have their phones switched on and with them at all times. As previously mentioned in this chapter, two different categories of mobile phone users have been identified, power users and low users (see 4.2.7 Different types of mobile phone users). Low users do not consider their mobile phone as an essential part of their life and tend to have pay-as-you-go contracts, whereas power users tend to have monthly contracts.

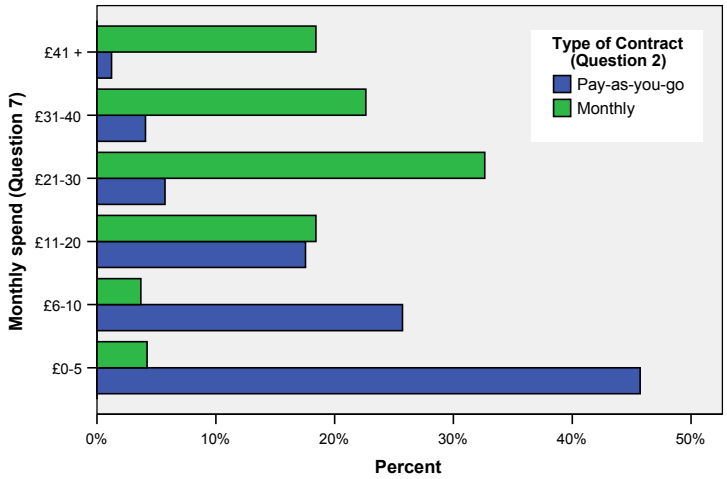


Figure 4.21: Associations between monthly spenditure (Question 7) and contract type (Question 2)

The survey data shows that pay-as-you-go users spend considerably less than those with a monthly contract (see Figure 4.21, above). At the same time, users with monthly contracts, consider their phone as very important and on average as more important than pay-as-you-go users (Figure 4.22, below).

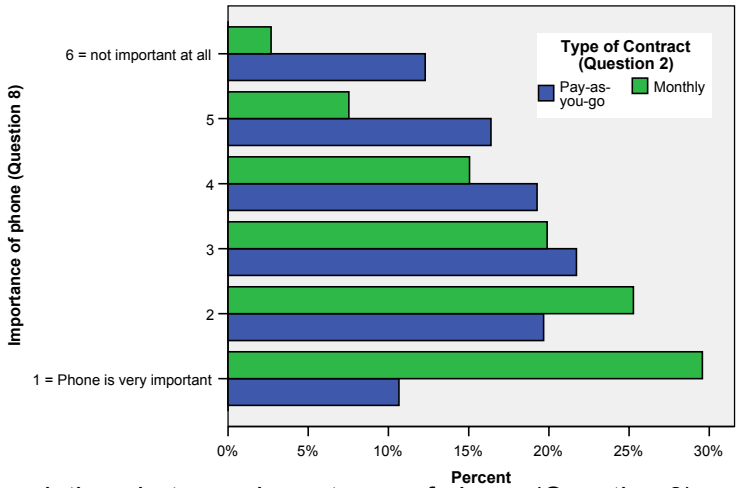


Figure 4.22: Associations between importance of phone (Question 8) and contract type (Question 2)

4.3.2.3 Differences in data collection phases regarding phone contracts and handsets

When comparing the data sets before and after the 07/07/05 terrorist attacks, differences regarding mobile phone use became apparent. The data sample collected after the London terrorist attacks in 2005 showed an increase in pay-monthly phone contracts (+13.6 percentage points), together with an increase in camera phones (+20.8 percentage points). Accordingly in the same time period, there was a decrease on pay-as-you-go contracts and black and white phones. The change in handsets is very likely caused by the increase of monthly paid mobile phone contracts, which tend to provide its subscriber with a new state-of-the-art phone.

4.3.3 Survey section B: Privacy and Personal Data

4.3.3.1 Respondents' definitions of privacy in the survey

The question ‘What does privacy mean to you?' (Question 9) was the only open question in the questionnaire (see section 3.4.7). Since the question allowed flexible responses, it was possible for a respondent to put forward more than one definition of privacy. A number of variables have been constructed to capture all responses and similar responses have been grouped together. Counts have been taken of the responses to indicate the strength of opinion or commonality of the experience. Higher counts suggest that an opinion is more common and hence possibly more relevant. The numbers should be taken as indicative as the responses were interpreted and quantified by the researcher and therefore researcher's bias cannot be ruled out.

The following variables have been set up to capture respondents' privacy definitions:
'Personal' has been referred to most (62 times); ‘control over information (50)’, ‘space’ (42 times) and ’security’ (41) were frequently referred to, as well as ‘communications privacy’ (38), which relates to statements regarding communications in general and others listening into conversations. 'Information privacy - access' (33) comprises statements about other people have access to individual’s data. Other responses were coded into the following variables: 'no intrusion' (32), 'information privacy in general' (31), 'solitude' (31), 'secret' (26), 'information privacy - no sharing' (23), 'no marketing' (19), 'surveillance' (18), 'others

not knowing what I am doing' (15), 'liberty' (15), 'data protection' (14), 'private vs public' (13) and ‘home’ (11).
A complete list of the variables, including examples, is shown in Appendix M - Survey Figures for all three data sets.

Parallels between survey findings and interviews (GT categories)

Respondents' privacy definitions supplied in the survey confirmed the privacy categories identified in the interviews (see section 4.2.10 Participants’ privacy definitions):

GT Category B: Participants’ privacy definitions
- Privacy is about my data and having control over it
- Privacy is about liberty and freedom of doing what I want
- Privacy is about space

A large number of respondents' privacy definitions provided in the survey related to ‘personal data’, ‘own information’ or ‘personal details’. The variable ‘information privacy’ has been created to capture these comments. Because respondents used terms relating to their personal data frequently and in different ways, sub-variables for ‘information privacy’ were introduced, such as 'control', 'access', 'no sharing', 'financial', 'ownership of data', 'storage', and 'misuse'.

Particularly, the following definitions of privacy provided in Question 9 confirmed the interview findings. For example, 152 references to 'information privacy' were made by 398 respondents, which confirms the relevance of the grounded theory Category B ‘Privacy is about my data and having control over it’ developed from the interview data (see Table 4.10, below). Tables 4.11 and 4.12 show survey variables relating to GT Categories A and C. The relationship between interviews and survey finding will be further explicated in the next chapter, Chapter 5 - Analysis of Findings.

Table 4.10: Survey responses relating to Personal data and control (Category B)

Variables relating to 'Privacy is about my data and having control over it' (GT Category B)	**Some examples of respondents’ comments about privacy** [numbers in brackets indicate questionnaire number]
‘Information privacy - control’ (mentioned 50 times)	“being able to choose what information is known about me” [Questionnaire no. 171], “Privacy – private – not for unwanted people to know about – personal to me and the people I choose to confide in” [431]

	"others not knowing personal information about you without your permission" [3] "my phone number is my property, I choose if I want to take calls " [217] "Organisation or acquaintance – who intrudes into my personal life without seeking my permission or following social etiquette" [190]
information privacy - access (mentioned 33 times)	- "no-one should have access to my personal data" [10], - "others not knowing or having access to information about me or my behaviour" [21]. - "Not available to everyone" [152] - "Privacy = I decide to whom and when access to me or my information is divulged" [193]

Variables relating to 'Privacy is about liberty and freedom of doing what I want' (GT Category B)	**Some examples of respondents' comments about privacy** [numbers in brackets indicate questionnaire number]
Liberty (mentioned 15 times)	- "Freedom to do what you want (legally)" [33] - "To do what one wants to do when one wants to do it without anyone else caring"[73] - "freedom to make decision without interference from outside influences" [172] - "comfort to behave in a manner I wish. [109] - "to be able to do anything I like when I like in private" [362]
'Others not knowing what I am doing' (mentioned 15 times)	- "No one knows what your are doing." [8] - "People not knowing what I do!" [25] - "Something which is told or kept on and a need to know basis with the person involved liable for this. (if you don't need to know, you are not told)" [67].
Space (mentioned 42 times)	- "a space where I can be uninterrupted" [233] - "my own space (mental and literal)" [47] - "personal space" [6], - "Not having your personal space invaded" [426]

Table 4.11: Responses showing indignation and resignation (GT Category A)

Responses indicating indignation and resignation (GT Category A)	**Some examples of respondents' comments about privacy** [numbers in brackets indicate questionnaire number]
Indignation and resignation (mentioned 7 times)	- "it doesn't exist - big brother is always watching!"' [127]. - "Masks - there is no longer. Privacy - but there is a crucial need to protect what safeguards we have, e.g. medical research" [Questionnaire 262] - "that our privacy is becoming more and more constricted. That it's claimed that this is for your own protection, but crime and terrorism still persist" [297]

Table 4.12: : Survey responses distinguishing between public and private space (GT Category C)

Responses distinguishing between private and public life (GT Category C)	**Some examples of respondents' comments about privacy** [numbers in brackets indicate questionnaire number]
Respondents distinguish between private and public life, between home and work life (mentioned 13 times)	- "Privacy of conversation, not wanting to hear other peoples conversations, using mobile phones in privacy, not in public spaces." [Questionnaire 437] - "Respecting my family life as opposed to my work life" [15] - "What 'privacy'? Today you have not any more a private life. You are reachable day and night. Working mobile (Phone, Computer, etc.) all over the world." [22]

4.3.3.2 Attitudes towards given views of privacy

After formulating their own thoughts on privacy, as described in previous section 4.3.3, respondents were requested to select privacy definitions out of a given list. These definitions were based on the pilot study findings and literature; several answers were possible. Numbers in brackets indicate the number of respondents, who have selected this definition, out of 477 total respondents:

Table 4.13: "Do any of these definitions correspond to your view of privacy?" (Question 10)

Answer option	Number of times selected
'No one having access to my personal data without my agreement'	422
'No one listening to my conversations'	367
'Privacy is about my home and my personal space'	365
'I can legally do what I want without feeling the need to tell anybody'	212
'Freedom from identification and from surveillance in public places'	158

Comments under the option 'Other' included "ability to block usage of records that have been collected about me." (Questionnaire 388) and "once electronic communications are used they are difficult to keep private intentionally/unintentionally" (Questionnaire 183).

The majority of respondents (88.4%) chose the definition 'No one having access to my personal data without my agreement' which confirms once more that respondents mainly associate personal data with privacy.

4.3.3.3 CCTV and loyalty cards

Respondents were asked to give their opinion regarding CCTV on a 6-point Likert scale. 79.2% of respondents chose the options 1, 2 or 3, which may suggest that the majority of respondents feel positive towards the use of CCTV cameras. Only 20.8% of respondents selected options 4, 5 or 6 which may indicate a sceptical point of view towards the use of CCTV cameras (see Figure 4.23)

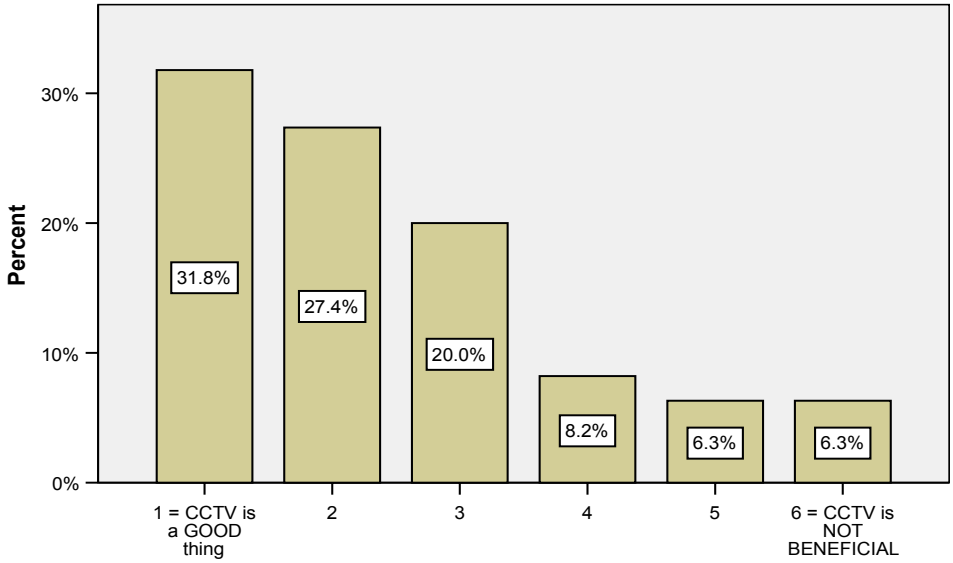


Figure 4.23: "What is your opinion about CCTV cameras on a scale from 1 to 6?" (Question 11)

When correlating the responses regarding CCTV use (Question 11) and whether it is beneficial to store location data for 12 months (Question 16), it became apparent that respondents who felt positive towards CCTV tended to approve of storing location data for 12 months (Figure 4.24). These results may indicate that those respondents, who believe in recording data for security purposes, do not make a distinction between CCTV pictures and mobile phone communications data (see also section 4.1.6.1).

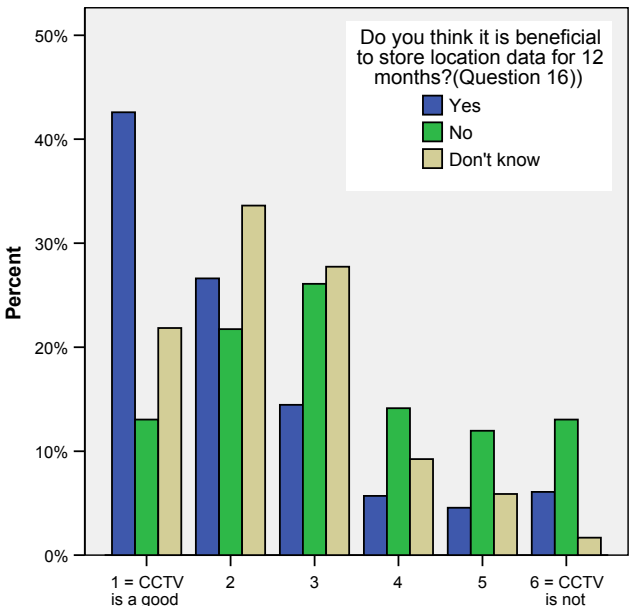


Figure 4.24: Association of attitudes about CCTV with data retention (Questions 11 and 16)

Another Likert scale was used to identify respondents' opinions regarding loyalty cards, commonly used by supermarkets or petrol stations. Options 3 and 4 were chosen most often, which may indicate that the majority of respondents felt indifferent towards loyalty cards or might not relate personal data collections to privacy (see Figure 4.25).

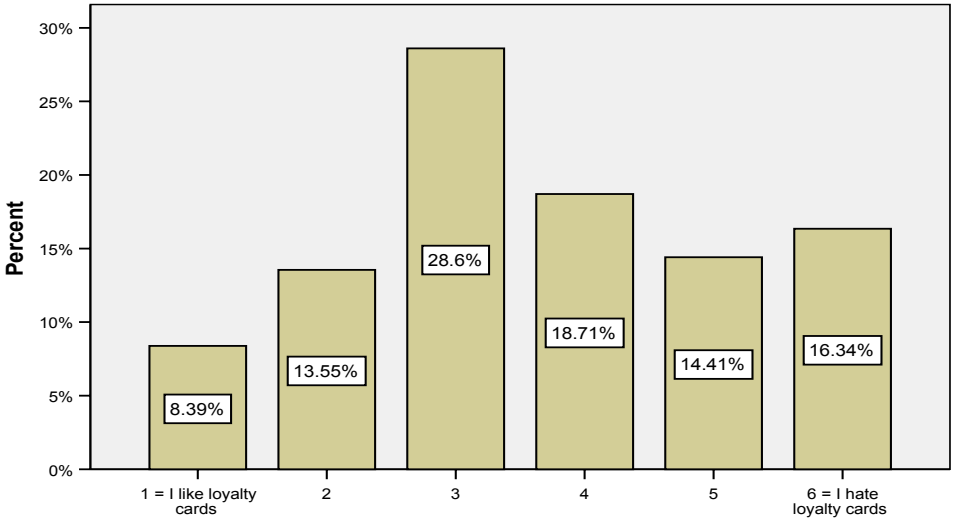


Figure 4.25: "What is your opinion on loyalty cards?" (Question 12)

4.3.3.4 Opinions towards popular privacy related statements

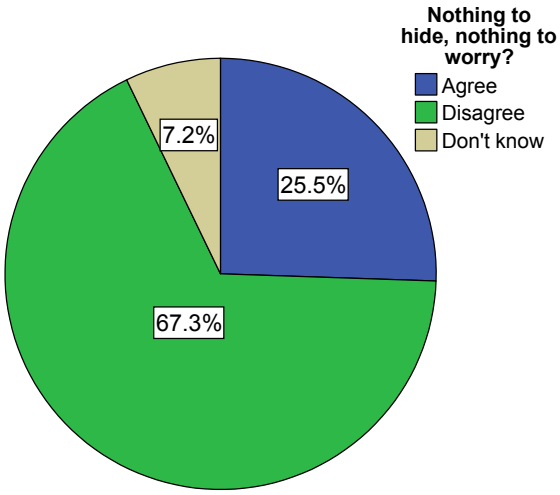


Figure 4.26: "People who have nothing to hide shouldn't worry about their privacy" (Question 13)

The majority of respondents (67.3%) disagreed with the statement "People who have nothing to hide should not worry about their privacy" (Question 13). A quarter of all respondents stated 'Agree' and only 7% selected 'Don't know' (Figure 4.26). These figures might indicate that a considerable majority of respondents believe in privacy, even though they have nothing to hide.

Only just over half of the respondents (54%) agreed with the statement "Giving up some privacy is necessary to fight terrorism and crime" (Question 14). About one third (31.1%) disagreed and 15% stated 'Don't know' (Figure 4.27). The percentage of those who selected 'Don't know' was twice as high as for the previous question (Question 13). The high percentage of those stating 'Don't know' could be seen as a confirmation of the 'Balancing act' that respondents have described in the interviews regarding security and privacy (GT Category E).

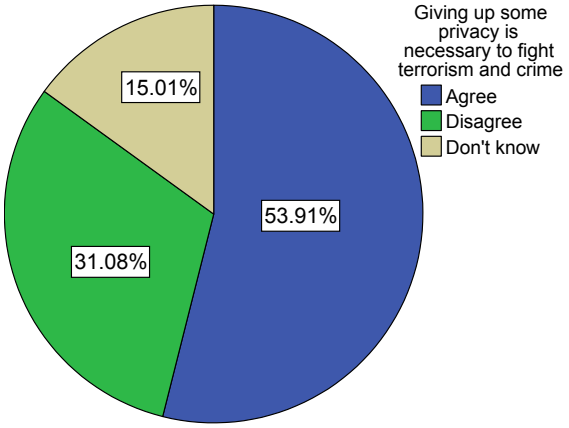


Figure 4.27: "Giving up some privacy is necessary to fight terrorism and crime" (Question 14)

4.3.4 Survey section C: Location Data and Legal Framework

The London terrorist attacks in July 2005 seemed to have influenced individuals' awareness of mobile phone location data. After the London terrorist attacks, the number of respondents who had 'Never heard of' location data fell significantly (by 12.8 percentage points.). In contrast, the number of those who said to be aware of the existence of location data increased. Those who claimed to have heard of location data increased slightly by 2 percentage points and the proportion of respondents who claimed to know about location data almost doubled (see Figure 4.28).

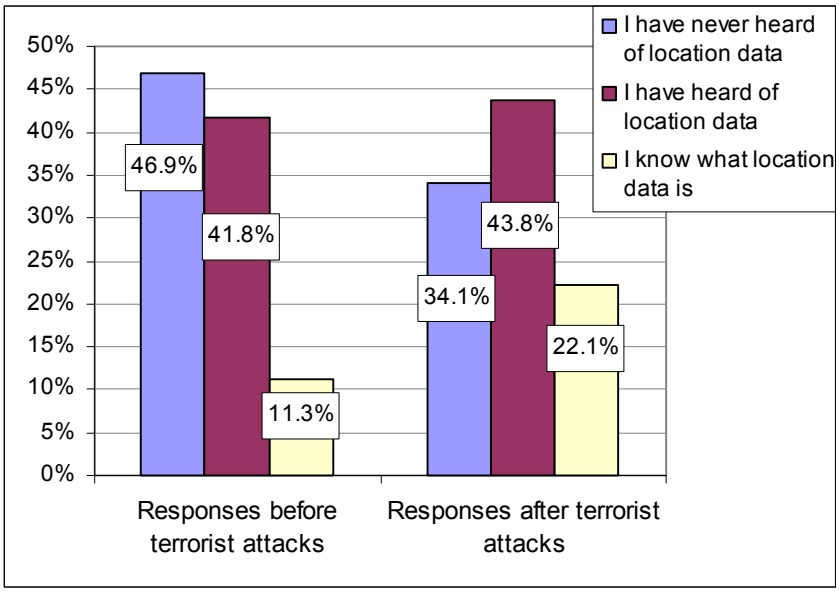


Figure 4.28: "Have you heard of location data before taking part in this study?" (Question 15)

Regarding the question “Do you think it is beneficial to store location data for 12 months for terror and crime prevention?” (Question 16), about half of the respondents (55%) agreed, a quarter of respondents (25.2%) stated ‘Don’t know’ and 19.5% stated ‘No’. Responses stayed similar across all data sets, which may indicate that the terrorist attacks have not had a significant influence on the responses to this question. A greater proportion of respondents stated 'Don't know' rather than 'No', which might point towards a lack of information that individuals have about the retention of communications data.

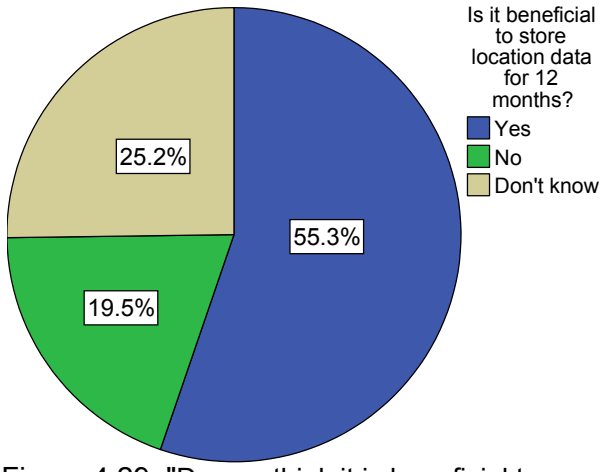


Figure 4.29: "Do you think it is beneficial to store location data for 12 months for terror and crime prevention?" (Question 16)

4.3.4.1 Concerns about data retention

A majority of 262 out of 477 respondents stated that they were either 'Not at all’ or ‘Not very’ concerned about data retention, compared to 195 who were ‘Fairly’ or ‘Very concerned’. This may indicate that respondents are in general not concerned about long-term storage of data.

In the next question, respondents could select several reasons for their concerns (Table 4.14). Most respondents were either concerned about not knowing *who* would have access to their data, which was selected by 180 respondents, or *how* the data would be used (172 respondents). Further concerns were expressed regarding not having *control* over data (131) and not knowing *what information* is held (138).

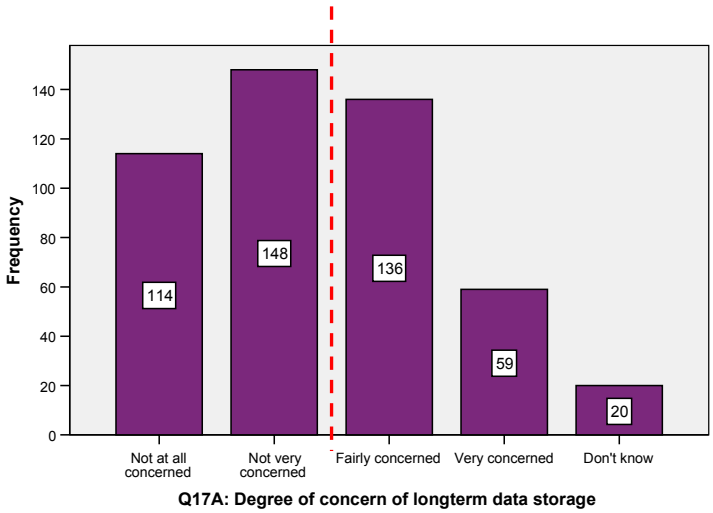


Figure 4.30: Concern about long term storage of location data (Question 17A)

Table 4.14: 'If concerned, what are your concerns?' (Question 17B), N = 234

	Don't know who has access	How will it be used?	What information is held	No control	No concerns	Other
Count	180	172	138	131	18	9

4.3.4.2 Respondents' perceived good uses of location data

The next question presented a list of suggested uses for location data to the respondents, out of which they could choose more than one response. The majority out of 475 participants who respondent to this question selected 'Emergency services' (429 times), followed by 'Solving crime' (355), 'Preventing terrorism' (314), 'Parents to track their children' (230). 'Employers to track employees' was selected by only 23 respondents (Table 4.15).

Table 4.15: Good uses for location data (Question 18)

	Emergency Services	Solving crime	Preventing terrorism	Parents for their children	Employers to track employees
Count	429	355	314	230	23

The responses to this question were similar across all three data sets with only minor changes in percentage points. After the London terrorist attacks, there was an increase for all answer options of Question 18, which was possible because several answers could be selected in this question. This may indicate that respondents could envisage many potential uses for location data, particularly for Terrorism (+9.2 percentage points), Children tracking (+5.1 percentage points) and Emergency (+2.5 percentage points). Table 4.16 shows details about the differences in results between data sets before and after the London terrorist attacks.

Table 4.16: Differences in data sets 'Good uses for location data' (Question 18)

	Before attacks	After 07/07 attacks	Change in percentage points
Emergency services	89.1%	91.6%	**+2.5**
Solving crime	74.2%	75.3%	+1.1
Preventing acts of terrorism	61.7%	70.9%	**+9.2**
For parents to track their children	46.0%	51.1%	**+5.1**
Employers to track employees	4.4%	5.3%	+0.9

4.3.4.3 Access to location data *without* mobile phone user's consent

A similar trend could be observed regarding respondents' views about the access of location data without their consent. Out of 477 respondents, 'Emergency services' was chosen the most often (352 times), followed by 'Police' (247), 'Intelligence services' (238), 'None' (75), 'Government departments' (23), 'Local councils' (10) (see Table 4.17).

Table 4.17: "Which of the following organisations should be allowed access to your location data without your consent?" (Question 19)

	Emergency Services	Police	Intelligence services	Government departments	Local Councils	None
Count	352	247	238	23	10	75

After the London terrorist attacks, the most significant changes consisted of an increase for Intelligence services (+ 12.8 percentage points), Emergency services (+ 9.1 percentage points), Police (+ 5 percentage points) and a decrease for 'None' (-6.7 percentage points).

Table 4.18: Comparing responses before and after London terrorist attacks (Question 19)

	Before attacks	After 07/07 attacks	Change in percentage points
Emergency services	69.8%	78.9%	**+ 9.1**
Police	49.6%	54.6%	+5
Intelligence services	44.0%	56.8%	**+12.8**
None	19.0%	12.3%	**-6.7**
Government departments	4.4%	5.3%	+ 0.9
Local Councils	2.8%	1.3%	-1.5

The responses to Questions 18 and 19 (Table 4.15 and Table 4.17) draw attention to the fact that respondents believe that location data should be best used for emergency services, followed by the purpose of fighting crime and terrorism. This confirms interview findings in that individuals comprehend location data primarily as a crime investigation tool (see section 5.2.1, Chapter 5).

4.3.4.4 Access to location data *with* mobile phone user's consent

When respondents selected who they would give access to their location data *with* their permission, several options could be selected. 'Family' was selected the most often (296 times), followed by 'Friends' (146), 'None' (127), 'Workplace' (41) and 'Commercial organisations' (12).

The option 'None' was chosen less often after the London terrorist attacks with a decrease in 9.2 percentage points. There was an increase of 8 percentage points for the option 'Family' after the attacks compared to before, as can be seen in Figure 4.31, below.

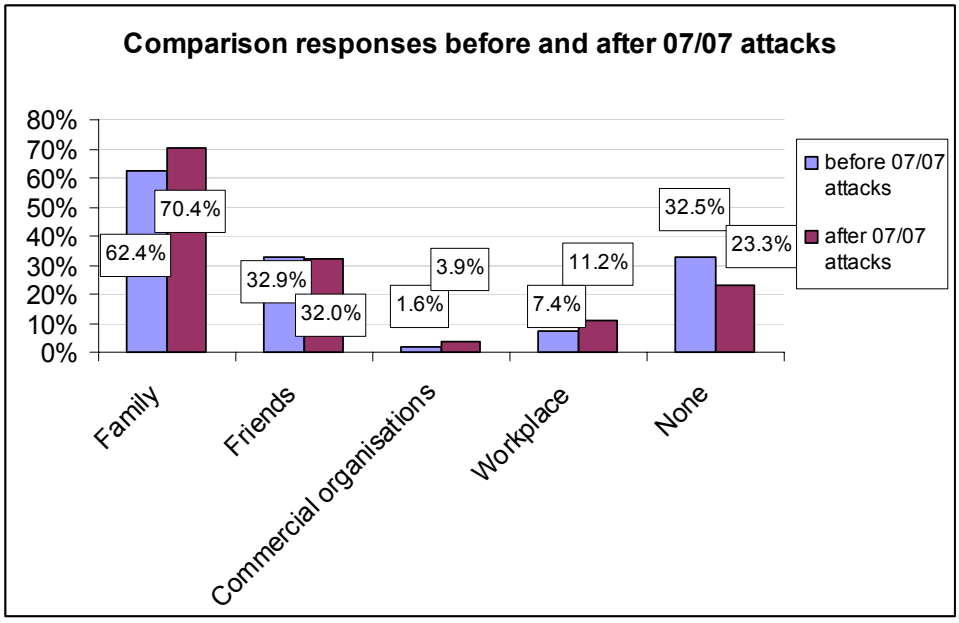


Figure 4.31: "Who would you allow access to your location data once you have given your consent?" (Question 20) - Comparison of responses before and after 07/07 attacks

Responses to Question 20 also correspond to findings from the interviews, as they show that respondents are very cautious about sharing their data with commercial companies, as they fear to be inundated with marketing material (see section 4.2.9.2). The fact that the option 'None' had been selected less often after the London terrorist attacks relates to the results described in section 4.3.4.2, in that respondents could see more beneficial uses for location data after the London terrorist attacks.

4.3.5 Summary of survey findings

This third and final part of Chapter 4 has summarised the findings from the survey. A relatively large sample of 477 respondents has helped to explore individuals' definitions of privacy and attitudes towards location data on a greater scale that it would have been possible with interviews. The London terrorist attacks, which occurred during the distribution phase of the questionnaire, appeared to have influenced individuals' responses regarding mobile phone location data. After the attacks, respondents showed an increased awareness of location data and at the same time could imagine more beneficial purposes for location data. Responses to the open question about privacy (section 4.3.3.1) predominantly referred to personal information and the desire to retain control over this data. Liberty and having the freedom to behave as they wished within legal boundaries was the other definition of privacy that was prominent in respondents' comments.

4.4 Chapter summary and conclusions

Mobile phone users' privacy should be at the heart of the debates about communications data retention. As it is their data containing specific information about their location and communications habits, that is being generated as a technological necessity and stored by default on a regular basis. For this reason, the views of citizens should have an influence on future policies regulating the collection, analysis and use personal data (Surveillance Studies Network, 2006), and hence this study has put considerable focus on the collection of empirical data. This fourth chapter has presented the empirical findings from all three data collection phases, which aimed at learning about citizens' awareness of location data and its impact on people's everyday lives. A detailed account of findings from the mobile phone location tracking pilot study, the in-depth interviews and from the survey has been provided. References to grounded theory codes, memos and visual representations of ideas have been made throughout this chapter, in order illuminate the process of developing the five final grounded theory categories.

The pilot study, in which the mobile phones of four participants were being tracked, has proven indispensable to render the abstract concept of location data visible to both the researcher and the participants. The first interview phase provided an initial insight into the participants' views and was followed up by more in-depth interviews that highlighted the status of the mobile phone in participants' lives. Furthermore, the interviews gave the researcher crucial insights into individuals' interpretations and perceptions of privacy in relation to mobile phones. Finally, the collection of further data in form of a survey helped the researcher to delve into issues raised by the interviews. The quantitative nature of the survey enabled the collection and analysis of data on a large scale and thus helped to process the data in a timescale feasible for a sole PhD researcher.

The subsequent chapter provides a discussion of the findings obtained from the three data collection phases. The chapter will highlight a number of parallels that can be drawn between survey data, interview findings and pilot study. Interpretations of the data are offered together with a comparison of empirical findings to the relevant literature.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 5 Discussion and Analysis of Findings: Divergent Perceptions of Privacy between Individuals and the Privacy related Literature

This analysis chapter has three parts. The first part makes explicit the relationships and connections between the grounded theory categories which were based on the interview analysis as presented in the previous chapter. The categories and their relationships are the basis of the grounded theory that offers an explanation about the phenomenon under study: individuals' views of privacy in relation to mobile phone location data. Each GT category is related to findings from the pilot study and survey, and this triangulation of empirical data and comparison to the relevant literature has helped to verify and strengthen the theory. The second part of this chapter presents four main findings relevant to the relationship between location data and respondents' perceptions of privacy. These originated from the categories and the connections that have been established between them. The third part of the chapter discusses divergences between the respondents' views of privacy and those commonly presented in the literature.

5.1 Part 1: Respondents' Views on Privacy

The main grounded theory categories developed from empirical findings are:

- GT Category A: Areas of privacy
- GT Category B: Participants' privacy definitions
- GT Category C: Contactability - Use of mobile phone to regulate privacy
- GT Category D: Perceptions of location tracking and power relationships
- GT Category E: Balancing (Core category)

5.1.1 GT Category A - Different areas of privacy relating to location data

Three areas of privacy were identified in participants' descriptions of privacy and these have been grouped into grounded theory Category A - Areas of privacy (see

section 4.2.9 for details). This GT category has served as a framework for analysing participants' statements about location data, as depicted in the following.

5.1.1.1 Privacy area of friends and family related to location data

The respondents did not perceive the potential access to their location data by family or friends as problematic. It was rather met with curiosity as to why someone would want to have access to information about their location. Survey results indicate that respondents would give access to their current geographical location in form of mobile phone location data to friends and family rather than to their workplace or commercial organisations. After the 07/07 terror attacks in London there was an increased consensus in giving location data access to family members in favour of not sharing location data with anyone (see section 4.3.4.4).

Respondents described as most important in this context the reasons for someone wanting to track a person's location. On the one hand, this confirms the existence of different areas in which privacy is important to participants. For example, because the participants taking part in the pilot study knew the researcher, they did not seem concerned about having their whereabouts monitored. As P117b_M explains:

> "Because if you were maybe a government body or something or something a bit more sinister then I think it might do. But as **it is just you**, it doesn't matter" (117_M).

On the other hand, P117_M's comments stress the significance of power relationships. Respondents want to know the motives for someone wanting to track them in order to be able to judge for what purposes the location data will be used (see GT Category D, section 5.1.5). In addition, these comments confirmed again that the control over personal data is important to individuals (see GT Category B, section 5.1.4).

5.1.1.2 Privacy area related to commercial companies

Interview and survey respondents expressed reluctance to give commercial companies access to their location data. In the survey, commercial companies were chosen the least for accessing respondents' location data, along with respondents' workplaces (see section 4.3.4.4). Respondents did not perceive any benefits for disclosing their geographical location to commercial companies but rather feared that they would be inundated with marketing material (see section 4.2.9.2). The balancing act of trading personal information with consumer benefits, such as

discounts, becomes particularly apparent in this context (see GT Category E, section 5.1.6).

5.1.1.3 Privacy area related to the government

The majority of interview and survey respondents had been aware of location data before taking part in the study. The London terrorist attacks in July 2005 seemed to have impacted on this awareness, as significantly more respondents stated to know about location data *after* the 2005 London terrorist attacks in comparison to before (see section, 4.3 Presentation of survey findings). Most respondents claimed to have heard about mobile phone location data from the media and primarily from radio or TV programmes about emergencies, crime or terrorism (see section 4.2.9.3).

Taking into account the respondents' apparent general awareness of location data, it could be deduced that phone users are also aware of *their own data* being retained by mobile phone service providers. However, statements regarding the uses of location data, indicated that very few respondents felt that location data in particular and mobile phone communications data in general did have any connection to their lives (see respondents' comments in pilot study, section 4.1.2.1, such as "I am not doing anything wrong" or "I am in public anyway"). Possible reasons for this may be that there are currently not many location-based applications or services available to citizens. Additionally, even though every mobile phone generates communications and location data, the mobile phone user does not see it, hence is not reminded of the data at any point in time.
It appears as if individuals only show an awareness of location data when specifically enquired about it. The reason for this may be that location data has not got a direct impact on their day-to-day activities and therefore individuals do not relate it to their own lives.

5.1.2 Responses to data retention

Respondents' comments and statements regarding communications data retention can be categorised as follows: firstly, *indignation* about not being informed about this retention of data, often in relation to with not feeling respected; secondly, *resignation* of users about having their data collected; and thirdly, *acceptance* of the retention of data because of crime and terrorist threats. Some respondents expressed all three attitudes towards data retention during an interview, which may indicate that they considered benefits and disadvantages of data retention from different view points in order to deal with the complexity of this subject area.

5.1.2.1 Expressing indignation in response to data retention

Statements about respect and wanting to be informed about the storage of mobile phone location data have been fielded into the sub-category 'indignation'. Respondents pointed out that the government should not have the *right* to track them without their consent. They wanted to be informed about collection of their data, and did not feel respected because of this. The respondents believed that they received very little information on the long-term data retention in the public media and in mobile phone contracts. With this in mind some respondents suspected that the government had a hidden agenda and could be hiding something (see section 4.2.9.3). For this reason, some interviewees suggested that the terms and conditions of mobile phone contracts should explicate that all communications data will be stored. This confirms GT Category B as it explains the respondents' perception that privacy is about data, the desire to have control over this data and who it is shared with or accessed by (see GT Category B - Respondents' definitions of privacy, section 5.1.4).

A survey of eight mobile phone high street shops at the end of July 2005 in Leeds city centre showed that shop assistants were not informed about current practices of the mobile phone service providers or the data retention legislation. In contrast to this seeming unawareness of the shop floor staff, the terms and conditions of the mobile phone service provider Vodafone provides the following information related to communications data retention:

> "10) Vodafone Limited and Personal Data
> a) **Personal data includes**: Call, network and traffic information generated by your use of the service covered by this Agreement or your use of products,

> services and content accessed via or facilitated by your use of the Services covered by this Agreement, including but not limited to the numbers you call, the type, date, time, **location**, duration and cost of calls, messages or other communications.“ (Vodafone, 2006)

Vodafone, one of the four mobile phone service providers in the UK, classifies ‘location’ as personal data and declares that this personal data may be used to “Comply with any legal, governmental or regulatory requirement imposed on us or in connection with legal proceedings” (Vodafone, 2006).

To summarise, the storage of communications data by service provider is referred to in the contract that every user signs, albeit in the small print where it is not straightforward to detect by consumers. In other words, customers of mobile phone service providers give their consent to the retention of their communications data by signing their contract.

5.1.2.2 Feelings of resignation

Several interview respondents expressed sentiments of resignation when talking about their communications data being accessed without their consent (see section 4.2.9.3). These feelings were mirrored when respondents provided their thoughts on privacy in the survey (section 4.3.3.1 Respondents' definitions of privacy in the survey). Their comments described the notion of resignation, potentially because respondents felt that they were not in control over personal data and unsure about who accesses their data and for what purposes.

5.1.2.3 Approving of data retention to fight crime and terrorism

Individuals describe a balancing act between privacy and security in each of the three areas of privacy identified: social, commercial and governmental (see Core category E, section 4.2.11). Particularly in the privacy zone related to the government, respondents point towards the conflicting roles of privacy and security (see section 4.2.9.3). In the interviews, respondents used expressions such as “balancing act” (P117_M), “grey area” (P133_M) or “double-edged sword” (P138_M) and these comments referring to a balancing act were again reflected in the survey data. For instance, the statement “Giving up some privacy is necessary to fight terrorism and crime” relates to the balancing act between privacy and security. More than half of respondents agreed with the statement and only less than a third disagreed (for details see section 4.3.3.4).

In the survey, most respondents showed little concern about the long term storage of their communications data by mobile phone service providers (see section 4.3.4.1). Instead, respondents identified many purposes for which location data could be used. As good uses for mobile phone location data were chosen: firstly, emergency services; secondly, solving crime; and thirdly, preventing acts of terrorism. These choices are identical to the organisations to which the respondents would give access to their location data without consent: firstly, emergency services, secondly, police and thirdly, intelligence services. All answer options relating to the three organisations and their services were selected significantly more often after the 2005 London terrorist attacks. At the same time the option 'none' was selected significantly less times (for details see sections 4.3.4.2 and 4.3.4.3).

5.1.3 GT Category C - Using mobile phone settings to regulate privacy in the social area of privacy

Mobile phones are an essential part of many people's lives in Britain. There are over 65 million mobile phone subscriptions in the UK, according to Ofcom (Mobile Operators Association, 2006). A comparison of this figure to an estimated UK population of 60.2 million (National Statistics, 2006) illustrates the widespread use of mobile phones in the British society - there is more than one mobile phone per British citizen. Other statistics suggest that more than 78% of households in Britain own at least one mobile phone (National Statistics, 2005). Findings for this study correspond to these mobile phone statistics, as 91 % of the 477 survey respondents owned a mobile phone.

The majority of mobile phone users taking part in the survey stated that they had their phone switched on and with them at all times. This was confirmed by the interviews, when individuals talked about routines and habits when using their mobile phone. In terms of communications data retention, this also means that, the location data generated by the participants' mobile phones are identical to that of the phone users' real-time location at most times. This raises the issue of individuals being traceable through their mobile phones at most or all times during the day and over a extended period of time, and confirms arguments voiced by human rights organisations that the continuous and routine retention of communications data subjects every citizen to the certainty of ongoing and unremitting interference in his or her private life' (Privacy International, 2003a). The richness of mobile phone communications data makes it possible to compile a detailed profile of a person's

interests and reveals sensitive information about a person's private life and social networks.

It was not one of the main aims of this study to identify different types of mobile phones users. Nevertheless, it soon became evident that respondents could be divided into two broad types of users based on the way they used their phones: Low users and power user (see section 4.2.7). The distinction between different types of phone users was confirmed by findings from the survey (see section 4.3.2.2). The two groups of phone users make use of their phone settings in different ways in order to establish a degree of control over how others can get in touch with them. This corresponds to regulating how others gain access to a mobile phone user, which in turn relates to individuals' perception and protection of privacy (see section 4.2.10.3), as the following comment shows:

> "You know one of the reasons why I necessarily won't have my phone turned on is because **I don't want people to be able to contact me all the time**. I don't want .. you know I want to have that .. **space**" (P134_F).

The mobile phone is mainly used to regulate access to a person relating to a person's social circle as explained in previous sections (see GT Category A - Different areas of privacy relating to location data, section 5.1.1).

Already in the 1960s, McLuhan has recognised the disruptive nature and potential of the telephone, which he describes as "an irresistible intruder in time or place" (McLuhan, 1964, p. 271). McLuhan makes this observation when talking about how effortless otherwise elusive managers can be reached by the telephone - a new technology in those days. The mobile phone can influence the way individuals manage time and space in their lives, as Green (2002) remarks. She points out that the use of technologies can help individuals to control time, which can result in spatial and temporal flexibility. The mobile phone can bridge distances and help the user to engage in work and social relationships irrespective of distance or location. The mobile phone can be used as a tool for "negotiating social relationships and conflicting roles in everyday life" (Green, 2002, p. 289). The GT Category Contactability (Category C), which was developed based on the respondents' statements, encapsulates this phenomenon as described by Green.

Geser (2004) claims that users gradually progress in using their phone over the time of phone ownership. He describes different phases of expanding mobile phone usage from emergency use to routine and more sophisticated use. Hence, this may

lead to the hypothesis that phone users adapt their ways of protecting their accessibility by others when changing their way of using mobile phone technology. However, it is not in the remit of this study to explore the long-term usage of mobile phones.

The Category C - Contactability supports claims that the mobile phone has become an inherent part of the citizens' lives (Harkin, 2003). However, this also means that mobile phone location data is collected about the mobile phone user on a continuous basis and irrespective of the place or the role that the individual holds in private or work life. As will be discussed in the following section, the mobile phone user's ability to manage and access personal data as advocated by data protection legislation is not achievable under the regime of blanket data retention. The data protection legislation had been developed to prevent harm to individuals and negative consequences on society, however, these protections have been significantly weakened as has been discussed in previous sections (see for example 2.3.3).

5.1.4 GT Category B - Respondents' definitions of privacy

The following sections interlink respondents' definitions of privacy as presented in the previous chapter (section 4.2.10) with survey findings and definitions from the literature.

5.1.4.1 Control over personal information

Participants of this study relate the notion of privacy to their personal data and express the desire to retain control over it (see section 4.2.10.1). Survey responses confirm these findings and draw attention to the different aspects of information privacy, such as ownership of data, control, access and preferences who to share data with (see section 4.3.3.1). In the survey, the statement 'No one having access to my personal data without my agreement' was chosen by the majority of survey respondents as the most suitable definition of privacy, and hence confirms the importance of personal data to individuals. In the interviews, respondents' describe a balancing act between telling others about oneself while at the same time retaining control over information that is communicated to others. The mobile phone as a ubiquitous communications tool can take the role as guard or as privacy protector by shielding the person from access by others, as explained by GT Category C (see previous section 5.1.3).

Respondents' thoughts about privacy regarding personal information and control correspond to what has been recognised by scholars for many years (see Chapter 2 - Literature Review, section, 2.1.2. What is worth noting here is that characterisations of privacy by participants seem to have remained similar to the rather traditional definitions, in spite of the increased use of digital data to store details about individuals (see section 2.1.4).

Mobile phone location data and control over information

It may seem remarkable that respondents' thoughts about privacy do not significantly differ from early privacy definitions by Warren and Brandeis in 1870. Especially as it could be argued that the relationship between privacy and personal data should have become more important *because of* the increased and routine generation of information facilitated by technological means. In other words, one could assume that definitions of privacy might change and adapt to technological developments.

Nevertheless, individuals do not ponder about the digitised processes of data collections and even more importantly the potential effects or consequences of those on their lives. For example, participants talk about keeping their information to themselves in relation to friends and family. However they do not mention concerns specific to the retention of communications data. This may seem startling considering that the mobile phone - one of today's most predominant means of communication - generates and enables the keeping of digitised data logs for all communication transactions over which individuals have very little control. A seeming paradox could be identified here between, on the one hand, control over information in a social context, and on the other hand, a laissez-faire attitude towards personal information in other contexts. This might find a part explanation in the different areas in life that individuals associate with privacy: friends/family, commercial and government (see GT Category A - Different areas of privacy relating to location data, section 5.1.1).

To summarise, despite the increased use of technologies in citizens' daily lives, respondents still refer to 'traditional' definitions of privacy, which are irrespective of technological influences and have been elaborated by scholars already many years ago. However, the increased use of digital technologies has an influence on citizens' *loss of control* over their personal information; in particular the generation of information and access to this information by others. Mobile phone location data

is a fitting example for this loss of control. Location data can be classified as information about the mobile phone user. It is generated in such a way that the mobile phone user does not have a *choice* over its generation, as the data is generated by default. Furthermore, the mobile phone user is often not aware of this data in everyday life and cannot know who accesses this data and for what reason. Hence the user cannot influence or *control* this type of personal data, which may lead to feelings of indignation or resignation (see 5.1.2 Responses to data retention).

5.1.4.2 Liberty and freedom of doing

On the one hand, it is important for individuals to retain control over their personal information, and on the other hand, it seems equally significant to them to not be controlled in the way they lead their life. Individuals' comments in the interviews tell of the desire to have the choice to do what they want within legal limits. Respondents' survey responses also confirm this notion of liberty and freedom (for more detail see section 4.3.3.1).

The empirical findings of this study relate to the philosophical work 'On Liberty' by John Stuart Mill, first published in 1859 (Mill, 1974).
P135_F's describes Mill's harm principle in her own words as follows,

> "(…) you generally treat everybody as you would want yourself to be treated. Then that's all that's matters to me. I don't see that what I do, ehm, unless it impinges on somebody else, affects anybody else" (P135_F).

Mill wrote that "Over himself, over his own body and mind, the individual is sovereign" (p. 69). The author has articulated the often referred to principle which states that one should do no harm to others. Related to this is the concept nonmaleficence, which requires avoiding doing harm and is an obligation in many moral theories (Chadwick, 2001).

Mobile phone location data and liberty

Some of Mill's beliefs from over a century ago, still correspond to the arguments that critics have raised in response to the current data retention regime (section 2.3.5). Mill talks about the "struggle between authority and liberty" and proclaims that the authorities need to be controlled by the liberty of the citizens, else the government can be a "dangerous weapon".

Individuals' desire for liberty is indeed related to the retention of mobile phone location data. It could be argued that *in theory*, the recording of location data does not affect or interfere with an individual's day-to-day activities because the generation and collection of communications data is not noticeable by the mobile phone user. Therefore the retention of communications data does not have an effect on their life or perception of privacy (see also P119_M's statements in section 4.1.2.2, Aim 2: Geographical location and privacy). *In reality*, however, the recording of a user's location data involves keeping evidence of a person's whereabouts; present and past. Location data can be combined with other communications data or information about the person. This pool of data can be compiled into a profile which conveys the phone user's habits and could also be related to the profiles of other persons (see section 4.1.1.5).

Following this, it is argued that a mobile phone user's awareness of the retention of communications data *may* have an impact on individuals' actions in everyday life (see also section 2.3.5.1 Objection on the ground of human rights and civil liberties). Respondent P133_M reflects on this relationship between perceptions of freedom and privacy as follows:

> "I just think like not my **personal freedom** in terms of like my freedom to do things but my perception of my freedom would change. Because, I might feel like I am being **tracked by something or somebody**" (P133_M).

In other words, the retention of location data may indeed have an impact on a person's freedom to make decisions about his or her actions and on how to lead one's life. In the same manner, the retention of communications data may prevent a person from partaking in communications with others or influence these communications, due to the person's awareness of a data log being taken of every communication. However, other findings suggest that mobile phone users rather forget about being tracked and hence it does not influence their behaviour (see section 5.1.5).

This study has focused on individuals' perspectives regarding the relationship between mobile phone location data and privacy, in order to identify how these compare to the positions of stakeholders such as NGOs, the British government or the academic literature. Despite this focus on a particular viewpoint, it is necessary to assess the potential impact of communications data retention on a person's freedom from a wider social context rather than merely a research participant's life. For one part, it can be argued that an individual's needs have to be balanced with

the requirements of the wider society (see situational map, section 4.2.2). For the other part, mobile phone data retention may have a potential impact on society as a whole. In other words, the behaviour of *one individual* may change in response to data retention. And this in turn would mean that if a considerable number of individuals change their behaviours, long-term data retention would have an effect on society as a whole.

To summarise, individuals describe personal liberty as an important element of their perception of privacy. The long-term retention of mobile phone location data can be seen as related to individual liberty, as its storage and use by various actors impacts on the interplay between individuals' needs and those of the wider society.

5.1.4.3 Privacy relating to space

Interviews and survey results indicate that respondents frequently relate privacy to the concept of space. On the one hand, they refer to ‘mental space’ in the sense of having the freedom to express oneself, which is related to the concept of liberty, as discussed in the previous section. On the other hand, respondents use the term space in the sense of territorial space, such as one's home, when defining privacy (see section 4.2.10.3). Survey respondents used the term “space” most frequently, after noting down “personal” and "control over personal data" when providing their own definition of privacy. Respondents make a distinction between private and public life, between home and work life, as highlighted by responses to the open question in the survey (see section 4.3.3.1). The privacy related literature defines the category of territorial privacy, which concerns the setting of limits on intrusion on physical space such as domestic and other environments (see also Territorial privacy in section 2.1.2.).

In addition to this, participants distinguish between different privacy related areas in their lives, as the interview and survey data indicate (see GT Category A, section 4.2.9). At the same time respondents' comments show that the mobile phone is a technology - potentially one amongst others - that blurs the boundaries between private life and work or public life. The phone user can be contacted, or in other words access to his or her personal space can be gained, whether at home, at work or at any other place. Hence, the distinction between different areas in life is not as uncomplicated as it is initially portrayed by some respondents.
Green (2002) confirms this observation of blurred boundaries by pointing out the shift from distinguishing between 'public' and 'private life' to the metaphors of 'on

time' and 'off time'. In other words, mobile phone users are reachable when the mobile phone is switched on, as opposed to having privacy when the phone is set to a less obtrusive ring tone setting or switched off, hence the expression 'off time' (see also GT Category C, section 4.2.8).

Mobile phone location data and space

Mobile phone location data is another case in point to illustrate the crossing of the imaginative borders between “my space” and that of “the others”, as 118_F discovers during the location tracking pilot study:

> A: Would you be concerned if the location service would be more accurate [than in the pilot study]?
>
> 118_F: yes.
>
> A: If it would show on a map what house you are in?
>
> 118_F: Mmh, not really.. what house.. yeah! Because it's my house. This sort of privacy if I am at home, no one should know where .. you know.. that's what we talked about: privacy. If it's government body, it's alright to know where I am. But other agencies, they shouldn't know where I am, if I am at home. But if I am in **public places**, like park or road, it is okay. **But then how will they distinguish between**, okay **where I am now**. How to differentiate between she's at **home** now okay we will leave her alone. That's the tricky thing, I think".

The mobile phone is a constant appendage to the majority of citizens, and mobile phone location data is generated and corresponds to a person's geographical location as long as a mobile phone is carried. This means that location data is stored whether the person is in a public space, at home or anywhere else - location data makes no distinction between different areas in life. Hence the storage of mobile phone location data does not distinguish between different territorial areas of space and therefore intersects private and public areas of a mobile phone user's life. In other words, mobile phone location data allows intrusions into traditionally private areas like homes. The only means that a mobile phone user has to avoid the transmission of location data is to switch off his or her phone (Harvard Journal of Law & Technology, 2004).

In addition, mobile phone location data contains information about a particular mobile phone user. As indicated in pervious sections (see GT Category B, section 5.1.4.1), it is important for individuals to keep in control over information about themselves, who it is shared with and accessed. This raises the question whether

location data retention also has an impact on an individuals' space in the metaphorical sense, in terms of liberty as discussed in the previous section 5.1.4.2.

This separation between public-self and private-self as described by respondent P118_F is also acknowledged in the literature (Nissenbaum, 1998). Others, such as Stalder (2002), warn that digital and ubiquitous technologies perforate the boundary between public and private life. This will be further discussed in part 3 of this chapter (section 5.3.4).

5.1.5 GT Category D - Perceptions of location tracking and power relationships

Respondents described a close relationship between who stores and accesses data about them and the potential uses, including misuses, of this data (see also section 4.2.3). The potential usages of personal data are particularly influenced by how much *power* the entity holds that has collected the data. Regarding location data and other forms of surveillance such as CCTV, respondents feel that the *use of data* is significantly more important, than the process or *act of being monitored*, as illustrated by Figure 5.1, below. Survey findings as presented in section 4.3.4.1 'Concerns about data retention', confirm that it appears to be most important for respondents to know *who* has access to the data, as this will have an effect on *how* the data will be used.

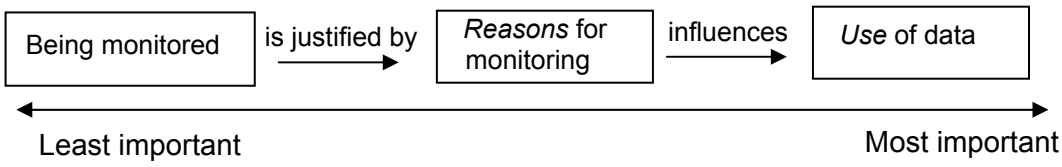


Figure 5.1: Steps in process of monitoring

All four participants agreed without hesitation to take part in the location tracking pilot study. They explained that they trusted the researcher to not misuse the data and to only make use of it for the study. In addition, all participants admitted in the final pilot study interviews to have forgotten about being tracked. This may be seen as an indication that the respondents did not feel concerned about neither the use of location data nor about being tracked by the researcher. An explanation for this may be that the researcher was known to the participants and hence part of their social privacy zone. She was therefore either trusted or not believed to have the capacity

to use the data for malicious purposes. In addition, it could be remarked that participants forgot about being tracked because it was not intrusive, hence they were not reminded of it. In this context, the claim of Blanchette and Johnson (2002) that the long-term retention of data results in the disappearance of 'social forgetfulness' seems to be particularly relevant. In contrast to human memory information technologies enable data to be recorded and never forgotten, which means that every action in the past can be recalled. And this may be an aspect of data retention that individuals can easily to overlook (see section 5.3). The authors believe that the value of social forgetfulness is a concept that allows individuals a second chance and is necessary for a democratic society, as "democracy is squelched when individuals live in fear of repercussions for any nonconforming behaviour" (p. 36). In contrast to this line of reasoning, it needs to be argued that it is necessary to hold information about individuals in order to make them accountable for their actions. Related to this are debates about data *retention* versus data *preservation*, which evolve around the question whether data for all citizens should be stored and if yes, for how long (see section 2.3.4).

5.1.6 Core category E - Balancing Act: Relationship between categories as a grounded theory about individuals' perceptions of privacy in relation to mobile phone location data

The following section summarises the relationships between the final categories and relates each of the categories to the Core category 'Balancing'.
The main grounded theory categories are:

- GT Category A: Areas of privacy
- GT Category B: Participants' privacy definitions
- GT Category C: Contactability - Use of mobile phone to regulate privacy
- GT Category D: Perceptions of location tracking and power relationships
- GT Category E: Core category 'Balancing'

All main categories are connected to the Core category 'Balancing' (see Figure 5.2). Privacy has a variety of meanings for participants, more than one for each participant. First, personal data and having control over it, second, liberty and freedom of doing what one wants to do and third, space (GT Category B). These meanings of privacy occur in particular areas and these include: friends and family, commercial companies, and government (GT Category A). Each of these three areas requires an act of balancing from the individual. Participants use mobile

phone settings to regulate their *contactability* or in other words their availability to others, mainly regarding their social contacts (GT Category C). Customers trade personal data against benefits from commercial organisations. Regarding the government privacy area, many respondents describe the need to balance privacy with security in the current political situation of terrorism threats (see section 4.2.12). Communications data, including mobile phone location data, constitutes data *about* a person. The data reveals a person's geographical location and communication habits whenever a mobile phone is carried and used. Findings from this study confirm that the vast majority of phone users carry their mobile phone at most times during the day. Many participants were aware of location data before taking part in the study. Some show feelings of resignation or indignation about having their data recorded without consent. Other respondents describe a balancing act between personal privacy and national security, which result in their acknowledgement of the need for long-term data retention to fight crime and terrorism.

Respondents of this study did not feel that they were under surveillance when their location data was recorded and stored by their mobile phone service providers and could have been accessed by governmental agencies; even if they understood that the data was being recorded. The actual process of having one's mobile phone communications data stored was not of importance to the participants but rather the *reasons* for the data collection (GT Category D). In addition, findings suggest that because the monitoring of location was not intrusive and happened without being seen by the participants, it did not seem to affect their behaviour. Factors such as fear, safety and convenience play a part, when determining whether data is stored for beneficial purposes. Of most importance to mobile phone users is the use of data, which once again highlights the relevance of personal data for individuals' perceptions of privacy. The GT Category D relates to the Core category 'Balancing' (GT Category E), in that the *use* of data is more relevant to respondents than the actual storage of location data. This could be interpreted as weighing up potential privacy invasions against the advantages of beneficial uses of data.

The debate about the balance between privacy interests, on the one hand, and wider societal and community obligations, on the other, has also been referred to by Bennett (1995, p. 7). He summarises adequately that "this debate raises central theoretical questions about the relationship between the individual and the state, about boundaries of public and privacy and about the essential contest between individual liberty and social values and concerns".

Figure 5.2, below, provides a graphical display of relationships between the main elements of the grounded theory developed from empirical data.

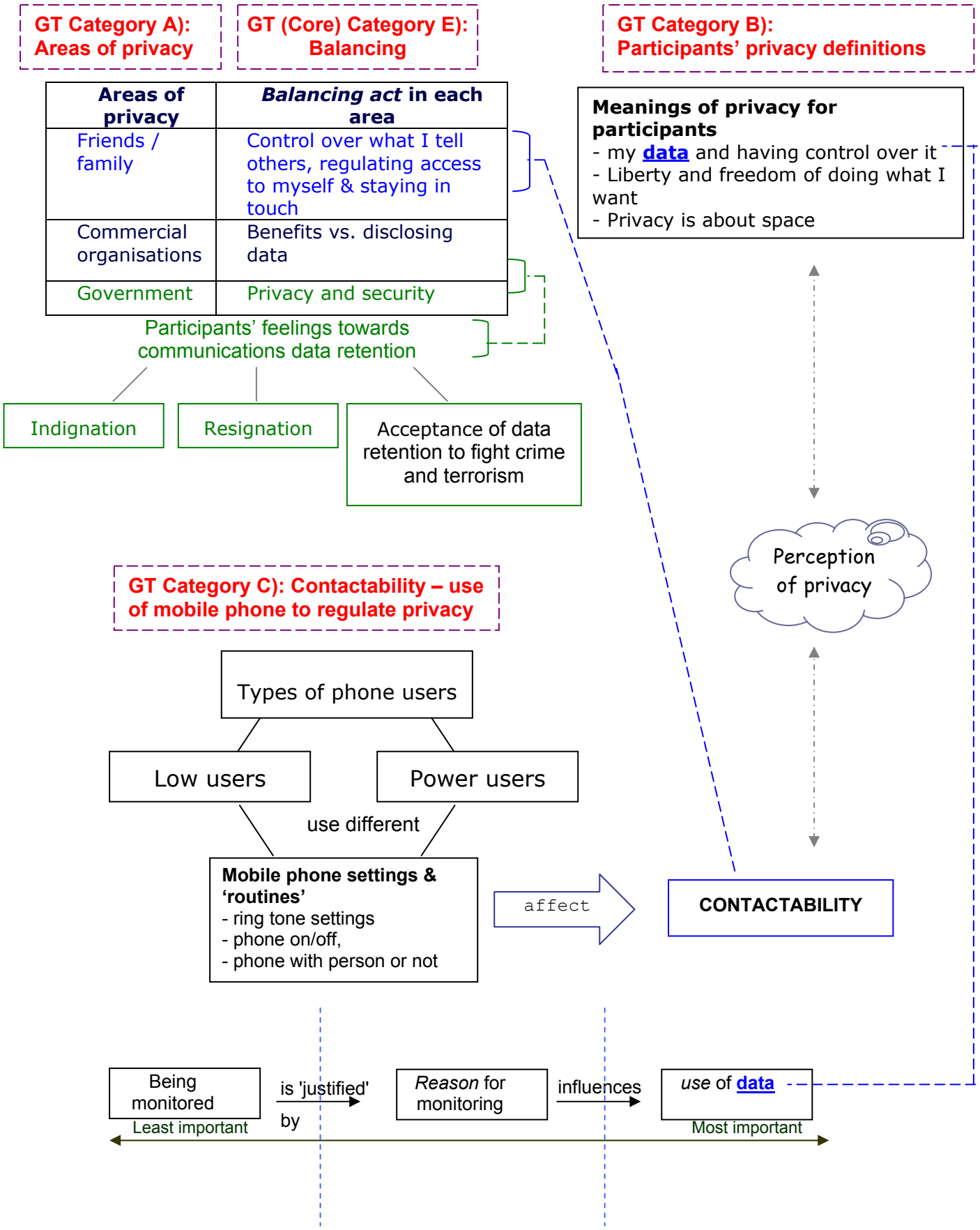


Figure 5.2: Relationship between Grounded Theory Categories

5.2 Part 2: Interpretations of Empirical Findings - Individuals' perceived Relationship between Mobile phone location data and Privacy

This second part of the chapter provides further interpretation of the empirical data and focuses on four main findings, which encapsulate the relationship between privacy and mobile phone location data. The findings are based on the GT categories, developed from pilot study, interviews and survey, as illustrated in part one of this chapter. The comparison between findings from this study and the privacy-related academic literature leads to the development of the main argument of this study (see section 5.3.3).

5.2.1 Finding 1: Location data is not a threat to privacy - it is primarily a crime investigation tool

The retention of location data in particular and communications data in general, is not perceived as a concern in terms of privacy for participants of this study.
The majority of participants claim in interviews and survey to have heard of mobile phones generating location data and that the data is used together with other communications data by police and intelligence services. This awareness of location data increased significantly after the London terrorist attacks whereas the number of those who stated to have *never heard of* location data fell (see section 5.1.1.3). At the same time, respondents describe privacy as being about personal data and the ability to exercise some sort of control over this data (see Category B, section 5.1.4).

Mobile phone location data can be seen as privacy invasive according to criteria identified in the literature (see section 2.1.2.1). Hence, it could be concluded that respondents either do perceive mobile phone location data as not personal *or* if they do, it is acknowledged that the data is useful to be stored in response to crime and terrorism threats. As highlighted by GT Category D (section 5.1.5), the reasons for retaining data are of most importance. Hence the retention of communications data for national security purposes is seen as a sufficient justification by respondents. Consequently, the majority of survey respondents believe that emergency services, police and intelligence services should be allowed access to location data without their consent.

It appears as if respondents perceive the potential misuse of communications data, such as profiling of citizens, as distant and abstract threats. In contrast to this, the need of emergency services or of the police to access communications data for citizens' protection is seen as more a tangible use of the data. The three privacy areas as identified by GT Category A support this idea. Predominantly the social area of privacy is important to individuals' perceptions of privacy. In other words the mobile phone user's immediate social environment and life style, associated with friends and family. However, mobile phone location data is seen to be linked predominantly to the government area of privacy, which is the most distant one to participants in terms of privacy. This may explain as to why the current long-term retention of communications data by service providers and its access by governmental agencies is not perceived as a threat to privacy by the majority of respondents.

Communications data is primarily understood as a crime investigation tool and because participants are "not doing anything wrong" (P119_M), they are not concerned about the storage of their data. In addition, they do not feel concerned about the storage of their communications data because they are just "one amongst a hundred and million other people" (P117_M). For these reasons, individuals believe that it would be unlikely for them to "be singled out" (P117_M) and become a victim of a miscount of justice.
Participants expressed only little concern about 'function creep' (Lyon, 2001), that is the use of data for another purpose than that for which it had been originally collected for. The respondents' views towards communications data retention may be called the "triumph of public interest" at the expense of privacy rights, as pronounced by Davies (1997, p. 161). There is a trade-off between privacy and security, or in other words, a desire of individuals to keep communications data private which needs to be weighed up against the efforts of the government to provide national security. This is detailed by the Core category 'Balancing' (see also 5.1.1.3 GT Category A - Privacy area related to government).

5.2.2 Finding 2: Location data is not related to day-to-day life

Even though individuals claim to be aware of location data in interview and survey, they do not relate this data to their day-to-day lives. This became particularly evident in the pilot study in which the geographical location of participants' mobile phones could be accessed by the researcher at any time. In an initial interview, the researcher had discussed the study with the participants. After the four week tracking period a final interview took place, in which all participants admitted that they stopped thinking about the researcher being able to access information about their real-time location.

This may on the one hand be seen as confirming the existence of different areas of privacy (see GT Category A, section 5.1.1). The researcher was known to the participants, hence, belonged to the friends and family privacy area. As explained above, communications data retention only affects the government zone of privacy, hence it has not an immediate effect on the life of mobile phone users and is hence not at the forefront of their minds. On the other hand, this may indicate that even though individuals claim to know about the existence of location data, they do not relate it to their personal lives. When they hear about location in the media, they see it as a crime investigation tool (see Finding 1, above). They do not realise that their own data is stored or they do forget about it, possibly because the phone has become as essential element of modern life. Individuals do not seem to think of the 'knock-on effects' of communications
data retention unless they make out visible consequences or particular media coverage.

The different views of privacy, as identified by this study correspond to those described in the Surveillance Study Network's report to the Information Commissioner (Surveillance Study Network, 2006). This report highlights three different views of individuals: first, the 'rational view', which corresponds to the justification of data retention as described in GT Category A, second the 'compliant, paranoid and powerless' reaction to surveillance, which ties in with this studies GT subcategories of 'resignation' and 'indignation'. The third view is described in the report as 'active' and depicts the views of the concerned citizen who is willing to participate in the debate about surveillance. However, this stance had not been clearly identified in this study's empirical data (see section 4.2.9.3).

This seeming discrepancy also relates to the concept of a privacy paradox as indicated by Stalder (2002). When citizens are asked questions about privacy, they claim to be concerned about it, however at the same time it can be observed that in everyday life they do little to protect it. The metaphor of a privacy gap is evoked by Viseu et al. (2004) to describe the same phenomenon. They provide the example that if requested to give out personal information, citizens provide it without asking further questions, as for example when asked about credit card application details on the street.
The fact that participants had forgotten about being tracked is also related to other findings from the pilot study (see section 4.1.2.3). Here the respondent P117_M explained that he was aware about his workplace keeping a log of email transactions and phone conversations. However, he would still use it for personal purposes as he frequently forgets about the potential of being monitored.

5.2.3 Finding 3: Beneficial uses for location data

Mobile phone location data does not currently play a role in respondents' day-to-day lives (see Finding 2, above). Even though an increasingly large number of respondents claimed to be aware of location data, no one mentioned to have used any of the commercially available services (see section 2.2.3 for examples of mobile location-based services). This corresponds to Finding 1, above, in that location data is predominantly perceived as a crime investigation tool.

Nevertheless, the survey data indicate that respondents could imagine several useful purposes for location data, particularly in the survey sample after the London terrorist attacks, in which more respondents claimed to know about location data. The majority of survey respondents stated that they would be willing to give access to their location data to family (70%) and friends (33%) and would give access to their communications data without their explicit consent, firstly to emergency, secondly to police and thirdly to intelligence services. And in correspondence to these figures the majority of respondents perceived the retention of communications data as useful (for more detail see Chapter 4 - Presentation of Findings, sections 4.3.4.2 ff.). When relating these findings to the GT categories, this means that respondents would share their location data within two out of three privacy areas as identified by GT Category A. For one part as a crime investigation tool in the government area, and for the other part with friends and family, however not with commercial organisations. Nevertheless, it could be expected that mobile phone

users would want to gain control over this data regarding their social privacy area, once location-based services will be more widely used in the UK. Otherwise there might the danger of their 'contactability' being compromised (see GT Category C, Contactability, section 5.1.3).

The participants explained in the interviews that they believed it to be beneficial that communications data was retained in response to terrorism threats. This also highlights the relevance of the GT Category D to describe individuals' attitudes towards location data and privacy - in that the *use* of location data is seen as more important than the actual *act* of being monitored. In addition, this also emphasises the importance of the Core category E 'Balancing' (section 5.1.6), because it was most important for respondents to know that location data was used for a beneficial purpose. This ties in with Lyon et al.'s (2005) claim that the wider social forces need to be taken into account when considering privacy issues. Particularly, as it can be desirable for individuals to supply and share their personal information, when this is beneficial for them. While Marx (2006) argues that contemporary "new" surveillance technologies (see section 2.2.5.1) are taken for granted by citizens and are seen as necessary for the "post 9/11 culture of control", which again helps to understand the view that communications data retention itself is not perceived as a means of surveillance, especially if it seen to serve a worthwhile purpose.

5.2.4 Finding 4: Location data enables creating profiles of mobile phone users

As explained in Chapter 2 Literature Review, continuous mass collections of digitised personal data can be interpreted as surveillance. These arguments seemed to be reinforced as even Britain's Information Commissioner terms Britain's society 'a surveillance society', based on the fact that the vast majority of citizens are subjected to frequent collections of personal data on a day-to-day basis (Surveillance Studies Network, 2006). Routine collections and potential analysis of data associated with individuals may be used for establishing profiles of individuals and populations (see section 2.1.5). Marx (2006) highlights as an important element of liberty a person's ability to control one's information and be unnoticed or rather noticed when one desires it. The capacity to control informational boundaries is necessary in civil society. The tendencies of bureaucratic organisations to want to amass more and more detailed personal information about individuals in order to react pro-actively to threats and risks. The literature on surveillance supports the view that quantity and quality of surveillance have changed. The volume of data

collected and stored by private as well as public actors has facilitated a range of new practices (Bennett, 1995).

It seems in stark contrast to these arguments that the majority of respondents of this study did either not seem to be *aware of,* or not *concerned about* these potential surveillance threats that are so often referred to in the popular and academic literature. Particularly the retention of mobile phone communications data bears the potential of identifying patterns in the collected data. Even if specific individuals are not identified, it is possible to analyse the behaviour of particular user groups or of mobile phone users located in a particular area (see section 2.1.5.1).

The pilot study confirmed the potential of location data to establish profiles of mobile phone users. The use of data from different sources helped to interpret incomplete data about a person and build a profile of a person's activities. The participants' geographical locations obtained by the tracking service provider were not accurate to the metre but only showed the postcode (see section 4.1.1.5). However, the researcher could on many occasions deduce a participant’s actual exact whereabouts by combining his or her approximate location with other known information about this person. Hence, it would have been possible to establish a complete picture of the person's movements and habits over time.

Findings of this study indicate that individuals often do not seem to be able to make out or notice digitised processes of data collections. Many pay attention to what is taking place in their own immediate environments, such as in their social area of privacy, or in other words regarding friends, family or work. However, communications data retention is only relevant to the government area of privacy and not any other of the areas associated with privacy (see Finding 2). The unawareness of collections of personal data inevitably leads to a loss of control over the generation and resulting usages of personal information (as described in section 5.1.4.1). Data protection and the lawful and responsible handling of data are essential when routine data collections take place for a particular purpose.
GT Category E (section 5.1.6) explicates the balancing act between the need for data collection with the actual use of the data.

5.3 Part 3: Individuals' Perceptions - Parallels and Divergences from the Academic Literature

Many stakeholders have debated the issues related to communications data retention as presented in the Chapter 2 - Literature Review (section 2.3.5). In order to examine the *individuals'* picture of privacy in relation to location data, this study has chosen an inductive methodological approach. This final part of the chapter illustrates similarities and variances between individuals' perceptions and those predominantly expressed in the literature.

Based on the empirical findings, as discussed above and in the previous chapter, two arguments have been developed:

> For one part, this study confirms existing definitions of privacy known from the literature. Respondents perceive privacy to be about personal information, control over it, personal liberty and space (see section 5.1.4 GT Category B - Respondents' definitions of privacy).
>
> For the other part, despite these similar and familiar privacy definitions, significant discrepancies can be identified between participants' views of privacy and the privacy related literature regarding the scope of privacy invasions and the use of technology.

Scope of privacy definition

Firstly, this study has identified that - perhaps not surprisingly - an individual's focus on privacy relates to and is based upon the individual's point of view, a person's *individual life*. Gestalt psychologists believe that individuals will always decontextualise data back into an individually defined whole or context in order to interpret it (Introna, 1997), which may explain the behaviour of the respondents of this study. Individuals describe the impact of retention of communications data on their life and do not to consider society as a whole which is, however, the predominant view in the literature. For example, individuals' definitions of privacy mainly relate to their personal data and not to the technologies that generate or handle the data. This may provide an explanation as to why participants do not see or not comprehend the impact of digital data collections, such as communications data retention or shopping loyalty cards, on a greater scale then their own immediate environment. Finding 2, above, supports this argument as individuals do generally not seem to be concerned about the retention of their communications

data and do not tend to relate this to themselves or to their own life. Also Marx (2006, p. 34) has found that individuals tend to "ignore the power of aggregating bits of data into a mosaic which is greater than the sum of the individual pieces".

In contrast to these views of the participants of this study, other academic literature predominantly focuses on the impacts of digital data collections on the society as a whole. The retention of mobile phone communications data of all British mobile phone users has an impact on the wider society as it can result in a climate of suspicion, threaten the freedom to speak and think freely (see section 2.3.5.1 Argument 1: Objection on the ground of human rights and civil liberties). The retained data can be accessed for every mobile phone user in retrospective and also may be used to make predictions for the future of individuals or groups of people with certain characteristics (see also Finding 4, section 5.2.4).

The notion of privacy influenced by technologies

Secondly, the respondents' privacy definitions mainly relate to *traditional* views of privacy, that is to say, they tend to be *independent of* technological influences. For the respondents of this study privacy is about moral rights and personal liberties. Threats to privacy are intrusions of personal space and also personal affronts associated with mass data collections, such as identity theft or annoying marketing calls. In summary, respondents' privacy definitions are about personal information and control, space and liberty (see section 5.1.4). Respondents do not perceive it as important that data is collected *per se*, as illustrated in GT Category D. Individuals describe that the uses of the data and who collects the data are the most important factors regarding personal data collections. For these reasons, it is argued that respondents' views of privacy predominantly relate to definitions of privacy in the literature that are not connected to new technologies or digital data.

When individuals talk about their views of privacy it seems that technologies do not play an important part (see Finding 2). What seems most relevant is the role of privacy in different areas in life (social, commercial, government). The mobile phone is a technological tool that helps to regulate access to a person, particularly in the area of privacy related to social contacts (GT Category C Contactability). However at the same time, a *blurring of boundaries* occurs between different areas in life such as private and work life *because of* mobile phones, which is to some extend recognised by individuals (see previous section 5.1.4.3 Privacy relating to space).

The literature, however, takes a different view of privacy compared to that of the individuals taking part in this study. Privacy literature published over the last decades - that is during the era of the so-called information society - predominantly focuses on the role of technology in relation to privacy. And particularly on the potential of technologies to invade the privacy of individual consumers and citizens, which in turn is argued to have an impact on society as a whole. Terms such as 'dataveillance' have been coined to describe the mass data collections of digitised data and the impact of this data retention on individuals *and society* (see section 2.1.5.2).

To summarise, two different views of privacy can be identified. For one part the predominant privacy definition of this study's participants which can be interpreted as corresponding to the traditional values of privacy, such as the "right to be alone" as postulated by Warren and Brandeis already in the late 19th century. This privacy definition will be referred to in the following as '*individual view of privacy'*. In contrast to this stands the '*collective view of privacy'* which can be predominantly identified in the more recent literature about privacy. This view of privacy relates to impact of technologies on privacy and the implications of these influences on the wider society.

These two distinct notions of privacy developed from the analysis of empirical evidence and its comparison to the literature lead to the following claim: A fundamental rift can be identified between the perceptions and definitions of privacy between individuals and the academic literature in relation to mobile phone location data. The depiction and recognition of this divergence is relevant as it can affect future policies regulating collections, storage and analysis of personal data. This discrepancy between *individual* and *collective* views of privacy is to some extent recognised by the participants of this study and also in the literature, as explained in the following sections.

5.3.1 Respondents' views regarding privacy, society and technology

Some interviewees pondered about the fact that they are one individual within the wider society, and the connection of this to mass data collections. The following quotes provide an example:

> "So, I don't think, I would be that bothered because I am not one of these people that worry about this **big brother state** they talk about. Because

> frankly in my thinking there is so many people out there anyway. **That I am just one person amongst a hundred and million other people**. So that's why I am not too bothered about being tracked, I don't think to be honest. And I think, **I do nothing wrong** anyway but" (P117_M).

> "You are just once more want part of like a **bigger picture** and you are like insignificant… individual, you are **just like a figure** or something (..)" (P136_F).

Some respondents grapple with the concept of being one citizen within the whole UK population. On the one hand this means to them, that they are one "insignificant" part of the overall "bigger picture" (see quote P136_F, above). On the other hand, this also suggests that they are very unlikely to be "singled out". In other words, they feel that it is very unlikely that their communications data will be scrutinised by the authorities. Particularly, as P117_M in the quote above points out that he is not doing anything wrong, meaning that he is not committing any legal offences that would require police investigations. The GT Category E ('Balancing Act') encapsulates this interplay between wanting to release personal information to be used for crime and terrorism investigations, and the desire to retain control over personal data.

Respondents often refer in interviews and survey to 'Big Brother' when talking about data retention (see Appendix M variable 'surveillance' in Question 9). In Orwell's novel 'Nineteen eighty-four', the fictional character Big Brother keeps the whole society under complete surveillance in order to punish those who rebel against the system (Orwell, 1959). Those being watched are kept subordinate by means of uncertainty which results in the situation that citizens can never be sure whether Big Brother is watching or not. This also relates to Jeremy Bentham's Panopticon prison plan; the Greek word Panopticon translates as 'all-seeing place'. In 1791, Bentham envisaged a prison layout which established control and power over inmates by subjecting the prisoners to the unseen and *potentially* constant gaze of the guards. No-one could be sure whether or not they were being observed (Lyon, 2001).
It can be argued for and against interpreting communications data retention as a version of surveillance similar to that described by Orwell or Bentham. On the one hand, there are parallels in that the retention of communications data can give mobile phone users the feeling that they are constantly under observation (see section 5.1.4.2). Mobile phone users do not have any means of determining whether their (present or past) data is being looked at or not, as the data is transmitted continuously and by default. On the other hand, individuals are often either not

aware of data collections, because they do not know about the long-term data retention or have forgotten about it (see Finding 2). This would mean that comparisons between the surveillance practices as imagined by Orwell or Bentham are not adequate, because most mobile phone users are *not conscious* of having their data collected and therefore do not feel monitored.

5.3.2 Individual and collective privacy in the literature

Phillips and Curry (in Lyon ed., 2003) describe three forms of privacy concern in relation to geodemographic systems. Geodemography is related to location data as it combines geography, the study of divisions of land according to latitude and longitude, with the demographics of the land's inhabitants. Geodemographic data can be used by commercial companies to target information towards those they want to influence; geodemographic segmentation classifies small areas with similar demographic profiles.

Phillips and Curry's analysis encapsulates privacy concerns articulated in other publications about personal space, mass data collection and private versus public data. Firstly, Philips and Curry recognise an invasion of personal space, which makes privacy a matter of individual rights and autonomy. Secondly, the authors identify privacy concerns in relation to corporate practices in the form of mass collections of consumer data. These can result in social discrimination through consumer profiling. Thirdly, the distinction between public and private issues, as also discussed by Nissenbaum (1998) (see also section 2.1). Regarding these three foci of privacy, Phillips and Curry identify different trends in social research over the last decades. In the 1980s scholars introduced the matter of *social discrimination* to privacy definitions. This opinion corresponds to Clarke's observations about the dangers arising from the systematic use of personal data stored in databases for the investigation or monitoring of individuals' actions (see Clarke, 1988, and also section 2.1), and therefore relates to the 'collective view' of privacy, as discussed above.

Furthermore, Phillips and Curry argue that the focus of privacy concerns has shifted in the 21st century towards the *personal affront* due to the increased use of mobile phones and PDAs which are carried by and assigned to one person. The mass collection and analysis of personal data, as well as discriminatory classification of individuals have moved into the background in favour of issues of trespass and

nuisance. This view corresponds to the privacy definitions of the respondents of this study, as it focuses on the individual view of privacy.

Phillips and Curry's accounts, and those of others support this study's claim that privacy definitions in relation to personal data can be divided into two distinct categories: firstly, privacy as an individual matter and secondly privacy on a collective level. The former focuses on individuals' perceptions of invasions of personal space, whereas the latter takes into account social dimensions and questions of social justice regarding data collections. Respondents of this study perceive privacy as an individual matter, independent of technology, whereas scholarly authors (such as Lyon, 2001; Stalder, 2002; and Marx, 2002) focus on the impacts of technology on privacy and tend to take into account wider social impacts of digitalisation of data deriving from use of technology.

5.3.3 Using GT categories to support the differing notions of individual and collective privacy

The distinction of two differing views of privacy as identified by this study and in the literature leads to the following argument. Whilst individuals still hold a rather traditional picture of privacy, not influenced by technology and solely related to their own personal lives ('individual privacy'), scholars paint a picture of privacy that is affected by technology and relates to society as a whole (‘collective privacy'). This observation is supported by the notion brought forward by Stalder (2002), proclaiming that many authors see recent developments in information and communications technologies as shifting the notion of privacy, away from a view focused on the individual towards a social concern on a wider scale. The study support this view proclaimed by Stalder but at the same time acknowledges that citizens' interpretations of privacy do not match up with this shifted concept of privacy.

The GT categories developed by this study (see Part 1 of this chapter) and the findings based on these categories (see Part 2) support the idea of a changing notion of privacy.

Grounded theory categories

The GT categories derived from empirical findings support the argument described above as follows: Privacy definitions of respondents correspond to the traditional views of privacy, not related to technologies (see GT Category B). Individuals’ views of privacy are predominantly related to the social area of privacy, in other words friends and family (see GT Category A). The mobile phone is a communications technology that can be used to negotiate and regulate privacy in this social area (GT Category C). Respondents explain that the actual process of personal data collection is not of relevance for privacy - whether facilitated by technology or not - but instead it is of particular importance who collects the data and for what purpose (GT Category D). In all three areas of privacy, there is a balance that needs to be struck between the reasons for data collections and its use, such as justifying communications data retention of all citizens with crime and terrorist investigations (GT Category E). It is important for individuals to know and agree with the reasons of data collection and to have trust in the entity gathering the data. Therefore it could be deduced that the *consent* of mobile phone users to store the data is not a relevant matter in this context. The mobile phone user's agreement with the long-

term communications data retention regime is provided when signing a mobile phone contract. In addition, it can be supposed that citizens would also give their explicit consent if required, as long as they would perceive beneficial purposes of data retention, such as for example benefits for safety and security.

Four main findings

To summarise, mobile phone location data is not perceived as a threat to privacy by participants because of its beneficial use by police, intelligence and emergency services (Finding 1). These uses of location data are not related to individuals' social area of privacy but to the government area of privacy. Hence location data retention is not perceived to be related to every day life (Finding 2). However, individuals could imagine beneficial uses of location data, in their social zone (Finding 3), in which case it could be expected that individuals would want to control location and other information related to themselves (GT Category B).

Despite location data seemingly not being related to an individual citizen's daily life, it is important to be aware of the potential of using communications data for profiling (Finding 4). Finding 4 particularly highlights the differing views of privacy between individuals and other stakeholders, the divergences between the concepts of 'individual privacy' and 'collective privacy'. Individuals still hold the traditional view of privacy and hence tend not to consider digital mass data collections as privacy invasive, despite the calls of caution by NGOs, academics and some of the popular literature.

5.3.4 Using a bubble metaphor to explicate the changing the definition of privacy in response to technological developments

A bubble metaphor as evoked by Stalder (2002) is particularly appropriate to further illustrate the divergences in privacy views of participants of this study and the literature. Stalder uses the metaphor of a bubble to illustrate and at the same time to criticise the commonly used definition of privacy related to personal data.

Privacy can be described as a bubble surrounding each person (see Figure 5.3). Size and dimension of the bubble differ from person to person and determine a person's ability to control who enters the bubble or in other words the person's personal space. This bubble metaphor relates to the notion of 'individual privacy', as described in the previous section, and hence corresponds to the research participants' definition of privacy: privacy is about personal data, space and liberty (GT Category B). According to this definition, privacy is an entirely individual matter and concern as opposed to relating to society as a whole.

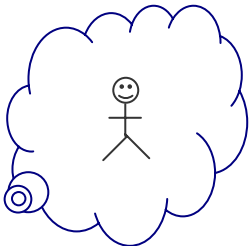


Figure 5.3: Privacy bubble surrounding a person

However, the findings from this study also confirm Stalder's claims that the bubble metaphor for privacy is not applicable for the following two reasons.

The first point of critique of the bubble metaphor is that a privacy definition according to the bubble metaphor would mean that *privacy protection is about defending a boundary between 'private' and 'public'.*

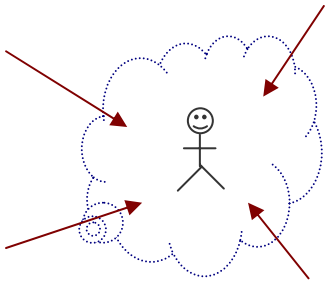


Figure 5.4: Privacy bubble is pierced by connections from the outside

The metaphor may be useful to illustrate the use of mobile phone settings to regulate access to a person, in other words to regulate access 'from the outside' by others. The phone acts as a shield, just like the bubble, to protect an individual's privacy (see GT Category C 'Contactability').

However, this boundary is not as rigid as the metaphor suggests, as modern life styles are often dominated by networked and communications technologies such as

the internet and mobile phones. These technologies pierce the bubble and result in numerous connections from and with the outside (Figure 5.4). Particularly the mobile phone pierces this imaginative protective shield in that it continuously collects and emits data about its user, such as for example in form of location data. New technologies challenge traditional barriers of privacy protection and physical means such as walls, distance or sealed envelopes and surpass physical limitations to information access (Marx, 2002). This study confirms that the boundaries between private and public have become blurred due to the use of mobile phone technologies (see in section 5.1.4.3, Privacy relating to space).

The second argument against the use of the bubble metaphor for describing privacy is based on the fact that the bubble metaphor assumes an *individual's ability to determine* who can access this individual's information and under what conditions. However, the numerous occurrences of automated collections of personal data facilitated by technologies, result in individuals not being able to exercise this control over the collection and use of their personal data. This also underlines the relevance of GT Category B, which identifies that privacy for the participants of this study is primarily about data and control over it.

On the one hand, the argument that individuals would not be able to control access to their data themselves seems questionable since most data collection occur repeatedly over time. Hence, decisions relating to data collections and data sharing do only have to be made once as to whether or not to release the data. On the other hand, many individuals are not aware of their data being collected, which relates back to Marx' accounts of new surveillance (see section 2.1.5.1). Additionally, individuals have not always got the choice to not release their data due to convenience, power relationships (see Chapter 4, Memo 1) or security requirements, such as CCTV. In addition, it is often desirable to be represented in certain databases, such as for example for credit ratings.
Because of the increased and automated generation of digital data about citizens and the use of this data for numerous purposes, it has become increasingly difficult for individuals to identify collections of personal data and react in an adequate way.

5.4 Chapter summary and conclusions

This chapter has provided an interpretation and analysis of the empirical findings from interviews, mobile phone location tracking and a survey. The grounded theory methodology was utilised to illustrate patterns and themes useful in understanding the broader discourses concerning location data relating to privacy, technology and policy-setting. The three data collection phases were at the heart of the study, as it was of vital importance to learn about and identify the perceptions and views of those whose mobile communications data is being gathered by default on a continuous basis. The grounded theory categories have been used to connect the empirical reality to the emerging theory.

The first part of the chapter has presented the grounded theory categories and the relationships between them to offer an explanation about the phenomenon under study: individuals' views of privacy in relation to mobile phone location data. A triangulation of empirical findings was successful in that pilot study and survey have confirmed the GT categories developed in the interviews. Findings from the empirical data were contrasted to the relevant literature in order to provide a holistic interpretation of the research question. The categories, relationships and the comparison to the relevant literature have resulted in the development of four findings, which have been presented and discussed in the second part.

Survey findings have shown that participants of the study were largely aware of the existence of mobile phone location data. Nevertheless, they tended not to perceive the long-term retention of mobile phone communications data and access by governmental agencies as a threat to privacy. Participants perceived different areas in relation to their view of privacy, as has been discussed in the grounded theory Category A (section 5.1.1). Privacy was seen to be mostly important to the participants' 'social zone', which mainly related to friends and family (see also Category C, section 5.1.3). Opposing to this zone closely associated with the concept of privacy, are dealings with the State and police. This area of privacy is the most distant one to respondents, as they tend to only deal with it on an exceptional basis, as for example in case of emergency or crime. The most significant of the four findings showed that the default retention of mobile phone location data was not perceived by respondents as a threat to privacy or a form of surveillance. Instead, location data was perceived as a crime-investigation tool, related to the

government area of privacy. Location data was not seen to be associated with the social privacy zone, as it was not seen to be related to day-to-day life, partly because it mobile users would not see any records of that data.

The third and final part of this chapter has drawn attention to the discrepancies between the respondents' views of privacy and those predominantly depicted the literature. It has been argued that the concept of privacy is changing with individuals' increased dependence on electronic communications technologies in everyday life. Whilst individuals tend to hold a rather traditional picture of privacy, not influenced by technology and solely related to their own personal lives, scholars paint a picture of privacy that is affected by technology and relates to society as a whole. Digital mass data collections, such as communications data retention, are not perceived as privacy invasive by individuals.

The subsequent and final chapter provides a set of broad conclusions and demonstrates how the aims and objectives, as introduced in Chapter 1, have been addressed throughout the thesis. Contributions to the field of studies and ideas for future research are presented and discussed.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

Chapter 6 Conclusions

This final chapter highlights the contributions of the PhD research to the field of study, but also considers the study's limitations. The aims and objectives, as introduced in Chapter 1, are revisited and addressed, as well as the criteria for grounded theory research. The chapter provides a conclusion for the overall study and makes suggestions for further research.

6.1 Contribution to the field and significance of the study

This research study has investigated the implications of mobile phone location data on individuals' perceptions of privacy. Citizens are being monitored in response to threats such as crime and terrorism and these growing collections of data may impact on individuals' civil liberties including privacy. The mobile phone can be seen as a very privacy invasive technology. It blurs the boundaries between different areas in life, such as family and work life. Mobile phone location data encompasses private and public spaces, and communications data is retained for ordinary citizens as well as for criminals. This study has taken to heart the call of researchers for more empirical studies investigating the impact of communications technologies on everyday life (see Chapter 1). Particularly the area of communications data retention has received very little empirical research interest so far. Rather prevalent are broad statements by the stakeholders involved (see Chapter 2, section 2.3.5).

The main contribution of the thesis is the development of a substantive theory grounded in empirical data from interviews, location tracking and a survey. This theory is specific to a particular area, as it maps the relationship between mobile phone location data and perceptions of privacy within the UK. The theory establishes links between concepts such as definitions of privacy and the process of monitoring. It explains how individuals use mobile phone settings as a way to regulate privacy, in other words, to regulate access to the mobile phone user.
Five final grounded theory categories were devised directly based on empirical data. The categories are as follows, 1) GT Category A: Areas of privacy, 2) GT Category B: Participants' privacy definitions, 3) GT Category C: Contactability - Use of mobile

phone to regulate privacy, 4) GT Category D: Perceptions of location tracking and power relationships, 5) GT Core Category E: Balancing.
By explicating the relationships between those categories, a theory about the phenomenon under study was developed. The theory explains that mobile phone users are predominantly aware of the existence of mobile phone location data and can imagine useful applications for this type of data. They do not perceive the retention of mobile phone location data as a form of surveillance or an invasion of mobile phone user's privacy but instead see the data primarily as a crime investigation tool. Respondents believed that the reasons for data being collected were more important than the actual act of being monitored, which emphasises the importance of the core category balancing which captures the balancing acts related to privacy that every individual needs to perform in everyday life.

Participants define privacy as being about personal data, control over it and personal space and liberty. Mobile phone location data can be identified as sensitive information about a mobile phone user. While the location information itself may not be privacy invasive, it may become so in conjunction with other data about the person and the potential to store this data for a long period of time. The data could be used to analyse past movements and communication routines of the person, as well as predict *potential* future behaviour, which can have negative consequences for the individual (see Chapter 2, section 2.2.5).

Findings from this PhD study support the argument that the concept of privacy is changing with individuals' increased dependence on electronic communications technologies in day-to-day life. This argument manifests itself in the divergence between the views of privacy in the literature and as expressed by the respondents of this study. The academic literature paints a picture of privacy that is affected by technology and relates to society as a whole. For instance, the literature tends to portray continuous collections of communications data as surveillance and hence as having an influence on the wider society as they can impact on social justice and civil liberties (see Finding 4, previous chapter). In comparison to this, individuals tend to hold a much narrower view of privacy, solely related to their own personal lives and tend to define privacy *independently* of technological influences. What seems important to them regarding privacy is their immediate social area, such as friends and family.

These views of privacy are reflected by individuals' attitudes towards mobile phone location data. Participants of this study did not perceive continuous collections of digitised data, such as mobile phone location data as a threat. A reason for this may be that the data and its uses do not seem to have an immediate and direct influence on individuals' lives. Location data is only seen as connected to the governmental privacy area (see Category A, section 5.1.1). Hence, location data or communications data in general are not perceived as a threat to privacy but primarily as a crime investigation tool.

Citizens' perceptions of the long-term retention of mobile phone communications data are of relevance - particularly the diverging views of individuals and the literature regarding the effects of data retention on privacy. The views of citizens can and should have an effect on future policies regulating the gathering, storage and analysis of personal data. For example, the Surveillance Studies Network (2006) has compiled a report for a conference hosted by the UK's Information Commissioner to address the implications of increasing surveillance and its impact on people's everyday lives. Hence, it is important to portray and represent the needs of ordinary citizens in this complex debate about technological influences on the privacy of individuals and the British society as a whole.

6.2 Limitations

The limitations of this study can be characterised as follows:

Firstly, it should be mentioned that the findings and analysis of this study are based on a limited number of respondents. A small number of ten interviews were conducted and the survey was completed by 477 respondents. In other words, the study's findings are based on a small sample and hence not generalisable across a large population. In response to this, it should be pointed out that it was not the aim of this study to conduct an entirely quantitative study with statistical validity. Instead, the grounded theory methodology was used to develop a small-scale or *substantive theory* to explain the phenomenon of individuals' privacy and communications data retention. Limitations of the GT methodology have been considered and addressed in Chapter 3 - Methodology (section 3.1.7).

Secondly and following on from the first point it could be seen as a limitation that only a small-scale theory was developed. This substantive theory focuses on the

explanation of a particular area, that is the relationship between mobile phone location data and individuals' perceptions of privacy in the UK.
A PhD thesis does not provide the scope and resources to raise this very specific theory to a more generalised level such as for example a formal grounded theory. This might be a possible undertaking for future research, as several substantive theories can build the basis for a more general formal theory.

Finally, it needs to be remarked that the author of this study was relatively new to using grounded theory methodology when conducting this research project. Hence it could be seen as a limitation that considerable time and resources were spent on learning how to analyse the data. However, this grounded theory research project has been a valuable learning experience that will help to carry out similar studies. In addition, the methodology had not been applied to the subject area of privacy, surveillance and mobile phone technology before. This study exemplifies that GTM can be a useful tool to study individuals' perceptions, not only in the 'traditional' GTM research areas of nursing and general health care.

6.3 Addressing the aims and objectives of this study

The main aim of this research project has been to investigate the implications of mobile phone location data on individuals' perceptions of privacy (see Chapter 1, section 1.3).

The objectives of the study were met as follows:
Chapter 4 (Presentation of Findings) has presented the results from an empirical investigation of individuals' awareness of and attitude towards mobile phone location data (Objective 1). The current technological and legal situation regarding mobile phone location data for the UK has been addressed in the literature review, Chapter 2 (Objective 2). The positions of stakeholders, such as the government, mobile phone service providers and individuals were addressed in the literature review in Chapter 2, and were supported by speaking to a desk officer for this dossier of the European Parliament, the Director of Privacy International and a spokesperson from Ofcom (Objective 3). The previous chapter, Chapter 5, has addressed and analysed the relationship between individuals' perceptions and the relevant literature regarding mobile phone location data (Objective 4). A theoretical model explaining the relationship between perceptions of privacy and mobile phone

location data has also been presented in Chapter 5 (Objective 5). This final chapter, Chapter 6, concludes the study and makes suggestions for further research.

6.4 Meeting the criteria of grounded theory

The grounded theory developed by this study is specific to the current and particular historical, social and local context, as captured in the situational map (see Chapter 4 - Presentation of Findings, section 4.2.2). Charmaz (2006) argues that placing a grounded theory in its particular social context strengthens it, as this enables comparisons between studies which can then be used to develop more abstract and general theories.

The findings of this study are specific to a time when the awareness of terrorism threats was prominent in the consciousness and lives of many British citizens. Hence, the findings have lead to the development of a substantive grounded theory, which is specific for a particular context, a particular area. The following section revisits the criteria for grounded theory studies, as presented in Chapter 3 - Methodology (see section 3.1.5).

6.4.1 Credibility

The criterion of credibility is about the links between theory and data, such as logical links between the empirical data, the main argument of the study and the analysis. For this study, a range of empirical data in form of pilot study, interviews and survey, were collected to develop the grounded theory. Open and focused codes were carefully devised for the interviews and the categories were developed based on the focused codes (see Chapter 4 - Presentation of Findings). Links between categories were explicated and have formed the basis for the grounded theory. Comparing the theory to the literature has helped to develop the main argument, as described in Chapter 5.

6.4.2 Originality

The criterion of originality assesses whether the categories developed in the study offer new insights into the area of research.
This study claims to be of theoretical significance because mobile phone location data has not been researched in relation to privacy using the grounded theory methodology. The finding that individuals see mobile phone location data as not connected to everyday life but mainly as a crime investigation tool sheds new light on the definition of and also protection of citizens' privacy (see Part 2 in Chapter 5).

6.4.3 Resonance

The grounded theory developed for this study portrays individuals' experiences with mobile phone location data in relation to their perception of privacy. The criterion of resonance aims at assessing whether the grounded theory categories developed from the data relate to the studied experience of participants and whether the categories make sense to them. Data collection and analysis for this study were conducted in alternating sequences in order to verify early findings and to shape further data collections (see section 3.1.2). In addition, the last three interviews (Interview phase 3, Appendix F) were used to present some of the tentative categories to the participants in order to evaluate how participants interpret them.

6.4.4 Usefulness

This criterion evaluates whether the analysis is related to individuals' day-to-day lives and whether it can be transferred to other areas than the one under study. A particular reason for using grounded theory was to learn how *individuals* perceive privacy in relation to mobile phone location data, as opposed to for example academic scholars or the popular media. For this reason, the empirical data collections for this study were aimed at capturing participants' feelings and opinions about the subject area and to let them express what is important to them in this context. Further research would be necessary to develop a more generalisable grounded theory that would be transferable to other subject areas (see section 6.6 Further Research, below).

6.5 Conclusions and lessons learned

Mobile phone communications data allows establishing a picture of a person's social interactions - who has communicated with whom, when and for how long. In addition, the user's geographical movements can be tracked, which makes the blanket retention of all users' communications data a new dimension in surveillance. The study has been of multi-disciplinary nature, encompassing the areas of mobile phone technology, privacy and legislation.

6.5.1 Mobile phone users' informational self-determination

The substantive grounded theory developed for this study has been based on the collection of empirical data. The five grounded theory categories, the relationships between them and the four main findings have been interpreted to provide an explanation for the phenomenon under study: the relationship between mobile phone location data and individuals' perceptions of privacy in the UK. Respondents of this study explained that it was important for them to be informed about collections of their personal data, otherwise they suspected a different agenda (see GT Category B, Respondents' privacy definitions). Some of the respondents did not consider themselves sufficiently informed about communications data retention, and therefore expressed feelings of indignation and resignation (see GT Category A). 'Compliant, paranoid and powerless with few rights' was a similar observation of views of surveillance subjects made by the Surveillance Studies Network (2006) in their report to the Information Commissioner. This may indicate a need for commercial organisations but also governments to sufficiently inform customers and citizens about the long-term retention of their data. However, despite these claims it needs to be recognised that the retention of mobile phone communications data, including location data, is in effect mentioned in the small print of every mobile phone contract (see Chapter 5, section 5.1.2.1). As has been argued throughout the thesis, it is increasingly challenging for citizens to make out collections of their digitised personal data, as these are often routine and embedded in the process of using technologies. However, as previously discussed in section 2.2.3.1, the European Court of Human Rights requires that surveillance legislation is sufficiently comprehensible, accessible and foreseeable, hence it may require further studies to ascertain that this is the case with data retention law.

Individuals fulfil different roles in their lives, which cross different social zones (see GT Category A, Areas of privacy). There are two main groups of actors to whom individuals' mobile phone location data is of interest for either commercial or for law enforcement use. Hence, the role of the mobile phone user regarding the retention of communications data differs from a legal point of view, depending whether it is defined as consumer or citizen (see section 2.2.7). For commercial purposes the permission to use the data needs to be explicitly obtained, whereas its use by governmental agencies is seen as a necessity to fight terrorism and crime and therefore implies consent. Respondents to this study described a balancing act irrespective of the purpose for which the location data was used (see GT Core Category E), which may raise concerns in terms of the respondents' superficial dealing with this very complex topic. Even though individuals are the subjects of surveillance, they seem to have a limited interest in the possible effects of communications data retention on human values, such as privacy. In addition, the focus on economic benefits on the one hand, and the trading between privacy and security on the other hand, raises concerns about the degree of informational self-determination that individuals are expected to exercise. As has been discussed in Chapter 5, individuals may not 'see' or be aware of the consequences of long-term routine surveillance. Indeed, as the interviews showed many respondents were unaware of the potential threats that the retention of communications data could have on privacy, human rights and other values.

Yet, this study argues that even if individuals are being informed about data collections, it is not always possible for them to keep track of who has access to their personal information. Particularly as they are often not able to appreciate the wider context in which their personal data are collected (see Finding 2). It is therefore concluded that the principle of informational self-determination as advocated in current legislations such as the British Freedom of Information Act, Data Protection Act and European Data Protection Directives is not entirely sufficient to ensure citizens' protection of privacy (see section 5.3). Individuals may be aware of communication data retention but tend not to relate it to their own personal lives. In addition, they do not have the capacity to influence data collections without restricting their liberty. The Surveillance Study Network (2006, p. 84) in his report to the Information Commissioner confirms the claims from this study stating that "only a minority [of individuals] are probably able to exercise self-help as fully as 'responsibility' might imply". Even though participants of this study wished to be 'let alone' as they had expressed in line with Warren and Brandeis'

early privacy definitions (see GT Category B), they seemed not be able to exercise sufficient controls over their personal data. Privacy had been defined by the study's respondents as being about personal data and having control over it. However, keeping in control over data is often impossible with the plethora of data collections taking place at an on-going basis, and the long-term retention of communications data is only one example of this. In addition, the only feasible way for individuals to circumvent this data collection is to not participate in electronic communications, which is not a valid option for reasons of convenience and practicality, and would infringe on a person's liberty and human right.

6.5.2 Communications data retention and human rights

The retention of communications data by service providers for longer periods than necessary for business purposes can be seen as conflicting with the European Convention on Human Rights Article 8 'Right to respect for private and family life'. The right to privacy as enshrined in the Convention has been brought into British legislation in form of the Human Rights Act 1998. As has been discussed in previous chapters, private life extends to the right to establish and develop relationships with other human beings (see for example the case P.G. vs United Kingdom, No. 44787/98, 2001). Nevertheless, this 'right to private life' (Article 8.1) may be compromised if seen as necessary under a range of exclusive purposes listed in Article 8.2 ECHR, such as national security. As communications data is retained to assure national security and support the fight against terrorism, European member states can implement the Data Retention Directive in accordance with Article 8 ECHR (see section 2.2.1).

Before the September 11 attacks there had been widespread criticism of the long-term retention of communications data. However, the attacks have been used in the UK and EU-wide to evoke a paradigm shift in storing and accessing this type of data. Hosein (2004) observes that after the United Kingdom failed to implement a data retention policy nationally, the focus shifted to the EU to allow the UK to pass such laws under European legislation. The introduction of the Anti-Terrorism Crime and Security Act 2001 in the UK, which regulates the retention of communications data, has produced some well-publicised debates. The legislative process for this Act merely took four weeks, which can be seen as an inappropriate length of time considering the complexity of the bill - such a short time span cannot allow for sufficient Parliamentary and public scrutiny.

It has been argued that blanket retention of communication data offends the core principle of law: the requirement of foreseeability. Citizens should be given notice of the circumstance in which the State may conduct surveillance, so that they can regulate their behaviour in order to avoid unwanted intrusions (Privacy International, 2003c). In contrast to this, it could be reasoned that the legislation allows everyone to foresee that their communications data will be recorded and retained for a certain period of time. However, concerns also need to be raised in terms of proportionality. The legislation does not make any distinction between different classes of people and this disproportionate interference in privacy lives cannot be seen to be necessary in a democratic society. The European Court of Human Rights has on numerous occasions decided on comparable cases involving governmental surveillance of its citizens and found those cases to be in violation with Article 8 ECHR. For example in the case of Rotaru v Romania (2000, App. no. 28341/95), the European Court of Human Rights decided that a violation with Article 8 took place, when the Romanian security services had stored information on Mr Rotaru's past activities as a university student. The court commented that "there has to be at least a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate", as the "indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is (…) evidently problematic". In the case of Klass and others vs Germany (1977 App. 5029/71) the Strasbourg Court ruled that "powers of secret surveillance" would only be used "under exceptional conditions necessary in a democratic society".

As mentioned above, the introduction of the data retention legislation in the UK was deemed to be in accordance with the ECHR, as the data is retained to support the fight against terrorism. In spite of this, one of the first proposals for the blanket retention of communications data by the National Criminal Intelligence Service (NCIS) was made on behalf of the police, HM Customs and Excise and others (see section 2.3.3.2). This suggested that the data was not merely intended to be used for terrorism prevention and investigation but also for criminal investigations (Walker, 2002). Indeed, the Regulation of Investigatory Powers Act 2000 specifies a range of agencies that hold the powers to obtain communications data, such as for example the Inland Revenue or the Department of Health. The wide array of organisations who may gain access to the data as well as the width of purposes specified in the RIP Act for which the data may be used, raises concerns of 'purpose creep' (see section 2.3.3.1). The data retention legislation permits a much

wider range of purposes, such as public safety, preventing serious harm or collection of tax, than those for which a warranted interception of a communication can be made in order to obtain the content of the communication (Davis, 2003). As explained in section 2.3.2, the content of communication is considered as more intrusive than information about the communication.

The legislation regulating data retention has been enacted in response to national security concerns and with serious opposition on the grounds of human rights infringements. For instance, the ATCS Act has been criticised as “the surely the most draconian legislation Parliament has passed in peacetime in over a century” (Tomkins, 2002). Communications data, including location data, should only be requested as part of investigations into clearly defined categories of serious crime and terrorism (Harkin, 2003). The use of communications data for purposes that only tangentially related to these types of investigations would also violate the third principle of the Data Protection Act 1998. Therefore, data retention legislation should be reviewed periodically, in order to assess whether the monitoring of citizens as a precautionary measure needs to be upheld.
Stalder (2002) advises to focus on the new landscape of social power and describes surveillance as a structural problem of political power. The government should be encouraged to put in place adequate safeguards so that the collected data cannot be misused. This is currently being carried out under the oversight of the Information Commissioner. The Office of the Information Commissioner is the UK's independent public body set up to protect personal information and promote public access to official information an independent agency. The retention of communications data is a form of personal data processing, and hence it is subject to the Data Protection Act 1998. Oversight of the 1998 Act is by the Information Commissioner (Home Office, 2003c, Section 29). The Office of Surveillance Commissioners (2003) provides an oversight of the conduct of covert surveillance by public authorities according to Parts II and III of the RIP Act (see section 2.3.3.1). Future policies must not only embed protection of data once it has already been collected but should also counterbalance the desire of governments to conduct excessive data collections, which monitor the vast majority of citizens at all times in case of an "investigatory rainy day" (Walker and Akdeniz, 2003, p. 162). Further studies are necessary to evaluate whether data retention can ultimately make a difference in terrorism and crime investigation and prevention. National data from states with and without retention schemes should be compared over time, in order

to assess whether blanket data retention is effective in fighting serious crime (Breyer, 2005).

The on-going policy debate highlights the importance for citizens to be informed about the implications that the use of communications technologies may have on their lives as well as on the overall society. The study's findings indicate that individuals tend to be occupied with the focus on their own day-to-day pursuits and may not necessarily consider the scope and impact of their actions on the wider society. This makes it necessary for non-governmental organisations and pressure groups to keep up their efforts to alert citizens of the consequences of routine and underlying 'dataveillance' (see section 2.2.5.2).

Increasingly citizens' daily lives involve some form of communications technology. This means that citizens are subjecting themselves to surveillance *by default*, as a log of all communications activities is retained indiscriminately, preventing users from avoiding such surveillance when using modern communications technologies. Therefore, it is important for citizens and pressure groups to demand accountability of those who collect data and whose power is enhanced by those data collections. The Surveillance Study Network (2006) stresses the power that citizens have to make a difference, to influence policy by questioning data collections and refusing to hand over their data for purposes that are not comprehensible to them.

6.5.3 Data retention as a response to risk

Information and communications technologies are an essential component of Western societies and provide a variety of opportunities to oversee activities that may potentially be of criminal nature. As has been discussed in the Introduction Chapter, a switch has taken place away from reactive policing of incidents to the pro-active management of risks. As the preceding section has indicated, one of the major points of dispute of the data retention legislation has been the wide range of purposes for which communications data may be used (see also section 2.3.5.5). The current trend of the risk society, together with the inherent uncertainty of mobile populations, advocates the pro-active management of risks which is greatly supported by the accumulation and subsequent analysis of communications data, including mobile phone location data (Zureik and Salter, 2005). The routine surveillance of digitised personal data aims at gaining more knowledge about those who may become part of future risks. The more knowledge of the risk can be obtained, the greater are the powers to reduce the risk. The routine surveillance of citizens' everyday actions and communications enabled by networked technologies

facilitates the categorising of individuals and populations with the aim to classify them in terms of potential risk. This is not only relevant in terms of communications data but also for other types of data generated by information and communications technologies. Other location-aware and networked technologies, such as Bluetooth, RFID and Wifi, raise similar issues which need to be addressed in order to sustain civil liberties such as privacy.

6.6 Future research

This PhD research project has the potential to be expanded regarding the following areas. Firstly, the *substantive theory* of the relationship between mobile phone location data and individuals' perceptions of privacy in the United Kingdom could be expanded to a *formal theory*, for instance by generating more far-reaching hypotheses. In other words, the theory could be made more widely applicable, as for example to other countries and cultures, or to other types of digital data related to location tracking, such as RFID tags or location identification via Wi-Fi.

Secondly, a future research project could specifically look at whether the findings from this study are transferable to other types of personal digitised data other than mobile phone location data. Mobile phone users claim to be aware of location data but do not relate it to their personal lives (see Finding 2). These findings *may* correspond to other types of personal data, which would mean that individuals are not able to identify different types of data collections and hence have lost control over their personal data on a large scale. According to the participants' definitions (see Category B) and those of the literature (Chapter 2), this would translate into a significant loss of privacy for the individual. This loss of privacy would take place without the individuals' clear awareness or without any power to influence these ongoing process of data collections and potential subsequent uses of this data. As explained in Chapter 2, Literature Review, these transactions and communications leave behind a trail revealing details about the users' activities. Indeed, profiles of this individual's habits can be established which can also be used to predict future behaviour based on historical (trans-)actions.

Thirdly, it would beneficial to expand the research to other European countries to identify European citizens' awareness and attitudes towards location data. If the study is extended, means of data collection should encompass interviews, questionnaires and focus groups. Particularly the questionnaire could be distributed on a larger scale that it had been possible for a sole researcher. This would result in a more representative and larger scale survey that enables the comparison of awareness of and attitudes towards mobile phone location data across several European countries. It may be of particular interest to look at countries that have not (yet) implemented CCTV and other means of surveillance technologies on such a wide scale as the UK.

In addition to these areas, a longitudinal programme of research could be initiated to investigate whether technological efficacy has an effect on attitudes towards privacy. Findings from this study show that low users tend to perceive mobile phones as a threat to privacy whereas power users do use the mobile phone actively to regulate their privacy (see Category C, section 5.1.3). As a result, different user groups could be targeted with different messages and advice to protect their privacy.
It has not been an aim of this study to evaluate whether communications data retention is a useful means for crime and terrorism investigation and prevention - this needs to be left for other researchers to scrutinise. Hence, it may be of value to carry out a study to evaluate how useful it is to store all mobile phone user's data, similar to a Dutch study by the Erasmus University (EDRI, 2005b). The European Union Directive 2006/24/EC advocates evaluating the current approach of data retention, and for this reason it would be important to conduct an independent, academic and comparative study to assess whether mobile phone communications data retention can be seen an effective approach for dealing with crime and terrorism.

Furthermore, the discussion of the various techniques with which location-based surveillance technologies can be interlinked, needs to be expanded. Technological devices, such as mobile phones are typically assigned to and used by one person and are carried for significant periods of time. These location-aware devices have the ability to communicate with one another without the need of intervention by its user, as for example via Bluetooth or RFID tags. The limitations of technology have been used by respondents to this study but also in the literature as a rational for

surveillance. Today's technologies do not always function flawlessly and failures to interlink data from various systems have acted as protection from surveillance. However, this may not be the case in future scenarios that may make the linking of for example mobile phone location data to ID card information possible. These developments raise concerns about the disconnected and fragmented elements of personal identity collections, where multiple agencies collect and have access to information about individuals in various contexts. In addition, growing divisions prevail between those who have the means to mitigate the effects of growing IT-based surveillance and those who do not, and the Surveillance Studies Network (2006) warns that this may raise tensions. As this study has confirmed, there is the danger that information flows are being predominantly invisible, and when citizens become aware of the potential for misuse, it may be too late “to put this technological genie back in a bottle” (Lloyd, p. 60).

Communications data can constitute an extremely valuable investigative tool, and most would agree that police and intelligence services should be provided with the best possible means to enable them to perform their vital work. However, the premise for the data protection legislation developed over the last decades had been to address the potential for misuses of data. Communications data needs to be held securely by service providers and also by the governmental agencies that obtain the data under the RIP Act. Security breaches in data storage and loss of personal data could result in significant changes in citizens' views of how their data should be stored and used. A recent example has occurred in November 2007, when two computer disks owned by Her Majesty's Revenue and Customs went missing which resulted in the data loss of millions of child benefit claimants. Instances of data breaches may impact on individuals' perceptions of privacy regarding communications data retention, and further research in this area would be valuable.

Thesis title: An analysis of the relationship between individuals' perceptions of privacy and mobile phone location data - a grounded theory study.

Andrea Gorra, Leeds Metropolitan University, UK
Comments sent to a.gorra@leedsmet.ac.uk would be most appreciated.

7 Bibliography

No author (2004) Who Knows Where You've been? Privacy Concerns Regarding The Use of Cellular Phones As Personal Locators. **Harvard Journal of Law & Technology**, Vol. 18, No.1, Fall 2004.

13th Annual Conference on Computers, Freedom & Privacy (2003) Plenary Session #9 Data Retention in Europe and America: Ian Brown, Marco Cappato, Henry Farrell, Maria Farrell and Cedric Laurant. 2003, 2.30 - 3.45pm. [mp3 file] Available from:<http://www.cfp2003.org/cfp2003/program.html> [Accessed 07 April 2004]

Accenture (2003a) **The Business of Privacy: Managing Privacy Issues Rationally, Proactively and Sensitively** [Internet] Available from <http://www.accenture.com/> [Accessed 18th November, 2003]

Accenture (2003b) **The Economic Value of Trust** [Internet] Available from <http://www.accenture.com/> [Accessed 18th November, 2003]

ACLU_American_Civil_Liberties_Union (2002) **Answers to Frequently Asked Questions (FAQ) about Echelon**. [Internet] Available from <http://archive.aclu.org/echelonwatch/faq.html> [Accessed 10th May 2004]

Agre, P., Rotenberg, M. (Ed.) (1997) **Technology and Privacy: The New Landscape**, London, MIT Press.

Agre, P. (1997) Beyond the Mirror World: Privacy and the Representational Practices of Computing. In: Agre, P., Rotenberg, M. ed. **Privacy and Technology: The New landscape** London, MIT Press.

Ahmed, K. (2000) Secret plan to spy on all British phone calls. **The Observer**, [Internet] Available from <http://observer.guardian.co.uk/uk_news/story/0,6903,406191,00.html> [Accessed 01 July 2007.]

Akdeniz, Y., Walker, C., Wall, D. (Ed.) (2000) **The Internet, law and society**, Longman, Harlow.

Akdeniz, Y., Taylor, N., Walker, C., (2001) **BigBrother.gov.uk: State surveillance in the age of information and rights**. [Internet] Available from:<http://www.cyber-rights.org/documents/crimlr.pdf> [Accessed 05 August 2006]

Ali, M. (n.d.) Survey of current location and positioning techniques. **The Institution of Engineering and Technology website** [Internet] Available from:<http://www.iee.org/oncomms/sector/communications/Articles/Object/9A36F175-2C5E-4EAC-91D62762AD6CE637 (login required)> [Accessed 21 December 2006]

Alvaro, A. (2005) **Report to Committee on Civil Liberties, Justice and Home Affairs - on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism** [Internet] Available from <http://www.europarl.europa.eu/registre/recherche/NoticeDetaillee.cfm?docid=130731&doclang=EN> [Accessed 10 July 2005]

Anti-Terrorism Crime and Security Act 2001 (ATCSA) [Internet] Available from <http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm> [Accessed 04 August 2006]

APIG (All Party Parliamentary Internet Group) (2003) **Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003** [Internet] Available from <http://www.apig.org.uk/archive/activities-2002/data-retention-inquiry/APIGreport.pdf> [Accessed 31 July 2006]

Article 29 Data Protection Working Party (2004) **Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]** [Internet] Available from <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf>. [Accessed 16 June 2006].

Article 29 Data Protection Working Party (2005) **Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM (2005) 438 final of 21.09.2005)** [Internet] Available from <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf> [Accessed 02 August 2006]

Bailey, S. H., Harris, D. J., Ormerod D. C. (2001) **Bailey, Harris & Jones Civil liberties : cases and materials**. 5th ed. Butterworths, London.

Bainbridge, D. (2004) **Introduction to Computer Law**. 5th ed. Pearson Education Limited, Essex.

Bartlett, D., Payne, S. (1997) Grounded Theory - Its Basis, Rational and Procedures In: McKenzie, G., Powell, J., Usher, R.,ed. **Understanding Social Research: Perspectives on Methodology and Practice** Falmer Press, London.

BBC News (2002) 'Snoop' plans raise privacy fears. 12 June 2002. [Internet] Available from <http://news.bbc.co.uk/1/hi/uk_politics/2037459.stm> [Accessed 05 August 2006]

BBC News (2006) **City-wide wi-fi rolls out in UK**. [Internet] Available from:<http://news.bbc.co.uk/1/hi/technology/4578114.stm> [Accessed 05 January 2006]

Beck, U. (1992) **Risk Society: Towards a New Modernity,** Sage Publications Ltd.

Bennett, C. (1995) **Privacy in the Political System: Perspectives from Political Science and Economics**. [Internet] Available from:<http://web.uvic.ca/polisci/bennett/pdf/westinbook.pdf> [Accessed 03 March 2006]

Bennett, C., Regan, P. (2004) Editorial: Surveillance and Mobilities **Surveillance & Society***.* Vol. 4, p. 449-455.

Bennett, C. (2005) What happens when you book an airline ticket? The collection and processing of passenger data post-9/11 In: Zureik and Salter,ed. **Global Suveillance and Policing - Borders, security, identity** Willan Publishing, Cullompton and Oregon.

Bennett, C., Crowe, L. (2005) **Location-based services and the surveillance of mobility: an analysis of privacy risks in Canada** [Internet] Available from <http://web.uvic.ca/polisci/bennett/pdf/LBSFINAL.pdf>. [Accessed 15 December 2006].

Beresfod, A. R. (2005) **Location privacy in ubiquitous computing. Technical Report, University of Cambridge, Computer Laboratory.** [Internet] Available from <http://citeseer.ist.psu.edu/cache/papers/cs2/445/http:zSzzSzwww-lce.eng.cam.ac.ukzSzlce-pubzSzpubliczSzarb33zSzUCAM-CL-TR-612.pdf/beresford05location.pdf> [Accessed 10 November 2006]

Bhogal, M. (2003) **United Kingdom Privacy Update 2003** Script-ed Issue 1, March 2004*,* [Internet] Available from <http://www.law.ed.ac.uk/ahrb/script-ed/docs/privacy_comment.asp> [Accessed 20th March 2004]

Blanchette, J., Johnson, D. (2002) Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. **The Information Society***,* Vol.18, pp 33-45.

Blaxter, L., Hughes, C., Tight, M. (2002) **How to research**. 2nd edition. Buckingham, Open University Press.

Blakeney, S. (2007) The Data Retention Directive: Combating terrorism or invading privacy. **Computer and Telecommunications Law Review***,* Vol. 13(5), pp. 153 - 157.

Blunkett, D. (2002) Civic rights. **The Guardian**, 14 September 2004. [Internet] Available from <http://www.guardian.co.uk/bigbrother/privacy/statesurveillance/story/0,,790138,00.html> [Accessed 18 May 2005]

Bowden, C. (2003) **Conversation with Caspar Bowden on the European Union Perspective on Data Protection** [Internet] Available from <http://www.microsoft.com/mscorp/innovation/twc/issuesissue2_intro.asp> [Accessed 8th April 2004]

Bradley, A. W., Ewing, K.D. (2007) **Constitutional and administrative law**. 14th ed. Longman, Harlow.

Breyer, P. (2005) Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. **European Law Journal**, Vol. 11, No.3, May 2005, pp. 365-375.

Bryant, A., Smit, J. (2000) **Grounded theory method in IS research: Glaser vs Strauss, Working Paper Leeds Metropolitan University** [Internet] Available from <http://www.leedsmet.ac.uk/inn/documents/2000-7.pdf>. [Accessed 11 February 2007].

Bryant, A. (2002) Re-grounding Grounded Theory **The Journal of Information Technology Theory and Application***.* Vol. 4, No. 1**,** pp.25-42.

Bryant, A. (2003) **A Constructive/ist Response to Glaser. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research [On-line Journal], 4(1).** [Internet] Available from <http://www.qualitative-research.net/fqs-texte/1-03/1-03bryant-e.htm> [Accessed 15 August 2005]

Cady, G., McGregor, P. (2002) **Protect your digital privacy - Survival Skills for the Information Age***,* Que, USA.

Casal, R. (2003) **Location and personal information for direct marketing: third generation killer application**. Info, 5(2), 45-50.

Caslon (undated) **Caslon Analytics privacy guide** [Internet] Available from <http://www.caslon.com.au/privacyguide4.htm> [Accessed 8th April 2004]

Cavoukian, A., Tapscott, D. (1996) **Who knows : safeguarding your privacy in a networked world***,* London : McGraw-Hill.

CDT - Center for Democracy & Technology (2006) **Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology** [Internet] Available from <http://www.cdt.org/publications/digital-search-and-seizure.pdf>. [Accessed 23 February 2005].

Chadwick, R. (ed.) (2001) **The Concise Encyclopedia of the Ethics of New Technologies**, Academic Press, London.

Charmaz, K. (2000) Grounded Theory - Objectivist and Constructivist Methods In: Denzin, N., Lincoln, Y,ed. **Handbook of Qualitative Research** Sage, Thousand Oaks, Ca., pp. 509 - 535.

Charmaz, K. (2002) Qualitative interviewing and grounded theory analysis In: Gubrium, J., Holstein, J.,ed. **Handbook of Interview Research: Context & Method** Sage Publications, London, pp. 675 - 694.

Charmaz, K. (2006) **Constructing Grounded Theory - A Practical Guide Through Qualitative Analysis**. Sage, London.

Clarke, A. E. (2005) **Situational Analysis: Grounded theory after the postmodern turn**. Sage, London.

Clarke, R. (1988) **Information Technology and Dataveillance**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html> [Accessed 21 February 2006]

Clarke, R. (1994a) Dataveillance by Governments: the technique of computer matching. **Information Technology & People***,* Vol. 7 No.2 1994, pp. 46-85.

Clarke, R. (1994b) **The Digital Persona and its Application to Data Surveillance**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html> [Accessed 27 June 2003]

Clarke, R. (1999a) **Introduction to Datavaillance and Information Privacy and Definitions of Terms**. [Internet] Available from <http://www.anu.edu.au/people/Roger.Clarke/DV/intro.html> [Accessed 23rd June, 2003]

Clarke, R. (1999b) **The legal context of privacy-enhancing and privacy-sympathetic technologies**. [Internet] Available from:< http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html> [Accessed 19 January 2007].

Clarke, R. (2000) **Person-location and person-tracking - Technologies, risks and policy implications**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html> [Accessed 24 April 2006]

Clarke, R. (2001) **Introducing PITs and PETs: Technologies Affecting Privacy**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html> [Accessed 19 January 2007]

Clarke, R. (2003a) **Wireless Transmission and Mobile Technologies**. [Internet] Available from <www.anu.edu.au/people/Roger.clarke/EC/WMT.html> [Accessed 19th January 2004]

Clarke, R. (2003b) **Mobile Technologies**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/EC/MTechno.html> [Accessed 22 February 2006]

Clarke, R. (2003c) **Dataveillance - 15 Years On**. [Internet] Available from:<http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html> [Accessed 22 February 2006]

Consumers' Association (2001) **Human Rights Act - What it means for you**. [Internet] Available from <http://www.which.net/campaigns/retail/cls/index.html> [Accessed 8th April 2004]

Corbin, J., Strauss, A. (1990) Grounded Theory Research: Procedures, Canons and Evaluative Criteria **Qualitative Sociology**. Vol. 13, No. 1**,** pp. 3-21.

Council of Europe (2001) **Convention on Cybercrime, ETS no. 185** [Internet] Available from <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. [Accessed 14 August 2007].

D'Roza, T. (n.d.) Overview of location based services. **The Institution of Engineering and Technology website** [Internet] Available from:<http://www.iee.org/oncomms/sector/communications/Articles/Object/9A36F175-2C5E-4EAC-91D62762AD6CE637 (login required)> [Accessed 21 December 2006]

D'Roza, T., Bilchev, G. (2003) An overview of location-based services. **BT Technology Journal**, Vol. 21, No. 1 January 2003, pp. 20-27.

Dandeker, C. (1990) **Surveillance, Power and Modernity**. Polity Press, Cambridge.

Danezis, G., Lewis, S., Anderson, R. (2005) **How Much is Location Privacy Worth?** [Internet] Available from:<http://infosecon.net/workshop/pdf/location-privacy.pdf> [Accessed 19 February 2006]

Daβler, T., Parker, D., Saal, D. (2002) Economic performance in European telecommunications, 1978-1998: a comparative study. **European Business Review**, Vol. 14, no. 3,, 194-209.

Data Protection Act 1998 (1998) [Internet] Available from <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm> [Accessed 04 August 2006]

Davies, S. (1997) Re-Engineering the Right to Privacy: How Privacy has been Transformed from a Right to a commodity. In: Agre, P., Rotenberg, M. ed. **Technology and Privacy: The New Landscape** London, MIT Press, pp. 143-166.

Davies, S. (1996) Big Brother: Britain's Web of Surveillance and the New Technological Order. Pan, London.

Davies, S. (2005) Unlawful, unworkable, unnecessary. **The Guardian**, 13 July 2005. [Internet] Available from <http://www.guardian.co.uk/attackonlondon/comment/story/0,,1527338,00.html> [Accessed 31 July 2006]

Davies, G., Trigg, G. (2006) BEING DATA RETENTIVE: A KNEE JERK REACTION. Communications Law, Vol. 11(1), pp.18-21.

Davis, H. (2003) Human Rights and Civil Liberties, Willan Publishing, Cullompton.

Denscombe, M. (2003) **The Good Reserch Guide for small-scale social research projects**. 2nd edition Open University Press, Maidenhead.

De Vaus, David (2002) **Surveys in Social Research**. 5th Edition. London, Routledge.

Deitel, H.M., Deitel, P.J., Nieto, T. R., Steinbuhler, K. (2002) **Wireless Internet & Mobile Business - How to Program**. New Jersey, Prentice-Hall, Inc.

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) [Internet] Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [Accessed 24 April 2006]

Directive 1997/66/EC - The Data Protection Telecommunications Directive (1997) [Internet] Available from <http://www.dataprotection.ie/viewdoc.asp?m=u&fn=/documents/legal/6aiii.htm>. [Accessed 27 March 2007].

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Internet] Available from <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf> [Accessed 24 April 2006]

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data (2006) [Internet] Available from <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf> [Accessed 04 July 2006]

Dunnewijk, T., Hulten, S. (2006) A brief history of mobile telecommunication in Europe, Working Paper Series [Internet] Available from <http://www.merit.unu.edu/publications/wppdf/2006/wp2006-034.pdf> [Accessed 01 October 2006]

EDRI European Digital Rights (2005a) **EP rejects data retention proposal. 15 June 05**. [Internet] Available from <http://www.edri.org/edrigram/number3.12/dataretention> [Accessed 20 June 2005]

EDRI European Digital Rights (2005b) **Dutch study fails to prove usefulness and necessity data retention** [Internet] Available from <http://www.edri.org/book/print/613s> [Accessed 07 August 2006]

Elliott, G., Phillips, N. (2004) **Mobile Commerce and Wireless Computing Systems***,* Pearson Education Limited, Harlow.

EPIC - Electronic Privacy Information Center (2007) **Data Retention**. [Internet] Available from:<http://www.epic.org/privacy/intl/data_retention.html> [Accessed 01 August 2007]

Ericson, R. V., Haggerty, K. D.(1997) **Policing the Risk Society**. Clarendon Press, Oxford.

Escudero-Pascual, A., Hosein, I. (2004) Questioning Lawful Access to Traffic Data. **Communications of the ACM***,* March 2004, Vol. 47, No.3.

European Commission (2002) **Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)**. [Internet] Available from:<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML> [Accessed 15 December 2006]

European Commission (2003) **The processing of caller location information for the purpose of location-enhanced emergency services (E112)**. [Internet] Available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003H0558:EN:NOT> [Accessed 11 December 2006]

European Commission (2006) **GALILEO: European Satellite Navigation System**. [Internet] Available from:<http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm> [Accessed 11 December 066]

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) [Internet] Available from <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf> [Accessed 04 August 2006]

European Digital Rights (EDRI) (2006) **Data Retention Petition Campaign,** [Internet] Available from <http://www.dataretentionisnosolution.com/> [Accessed 02 August 2006]

Foundation for information policy research (2003) **FIPR response to the access to communications data consultation** [Internet] Available from <http://www.fipr.org/030603access.html> [Accessed 02 August 2006]

Frankfort-Nachmias, C., Nachmias, D. (1996) **Research Methods in the Social Sciences**. 5th ed. London, Arnold.
Freedom_of_Information_Act_2000 (2000) [Internet] Available from <http://www.hmso.gov.uk/acts/acts2000/20000036.htm> [Accessed 15th December 2003]

Freedom of Information Act 2000 (2000) [Internet] Available from <http://www.hmso.gov.uk/acts/acts2000/20000036.htm>. [Accessed 15th December 2003].

Garfinkel, S. (2001) **Database Nation: The death of privacy in the 21st century**. O'Reilly & Associates, Inc., Sebatopol.

Garfinkel, S., Spafford, G. (2002) **Web security, privacy and commerce***,* Sebastopol, CA ; Cambridge, O'Reilly.

Gaspar, R. (2000) **NCIS Submission to the Home Office; Looking to the Future: clarity on Communications Data Retention Law** [Internet] Available from <http://cryptome.org/ncis-carnivore.htm> [Accessed 10 July 2007]

Gauntlett, A. (1999) **Net spies : who's watching you on the web***,* Satin Publications Limited, London.

Gavison, R. (1980) Privacy and the Limits of Law, **Yale Law Journal**, Vol. 89, pp. 421 - 428.

Gellman, R. (1998) Does privacy law work? In: Agre, P., Rotenberg, M. ed. **Technology and Privacy: The New Landscape** MIT Press, Cambridge, pp. 193 - 218.

Glaser, B. (1978) **Theoretical sensitivity : advances in the methodology of grounded theory**. Sociology Press, Mill Valley.

Glaser, B. ed. (1994) **More Grounded Theory Methodology: A Reader**. Mill Valley, Sociology Press.

Glaser, B. (2002) **Constructivist Grounded Theory? Forum Qualitative Sozialforschung / Forum: Qualitative Social Research [On-line Journal], 3(3).** [Internet] Available from <http://www.qualitative-research.net/fqs-texte/3-02/3-02glaser-e.htm> [Accessed 05 June 2006]

Glaser, B., Strauss, A. (1967) **The Discovery of Grounded Theory - Strategies for Qualitative Research**. New York, Aldine de Gruyter.

Global Internet Liberty Campaign (2002) **Letter to European Parliament** [Internet] Available from <http://www.gilc.org/cox_en.html> [Accessed 04 August 2006]

Gow, G. (2004) **Pinpointing Consent: Location Privacy, Public Safety, and Mobile Phones** [Internet] Available from <http://www.fil.hu/mobil/2004/Gow_webversion.pdf> [Accessed 6th May 2004]

Gow, G. (2005) Information Privacy and Mobile Phones. **Convergence: The International Journal of Research into New Media Technologies**, Vol. 11, No. 2, 76-87.

Gow, G. (2005) **Prepaid Mobile Phones: the Anonymity Question**. [Internet] Available from:<www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/gordon_gow.pdf> [Accessed 14 May 2006]

Graeff, T., Harmon, S. (2002) Collecting and using personal data: consumers' awareness and concerns. **Journal of Consumer Marketing**, Vol. 19, No.4.

Green, N., Smith, S. (2004) 'A Spy in your Pocket'? The Regulation of Mobile Data in the UK. **Surveillance & Society**. Vol. 1, issue 4, pp.573-587.

Green, N. (2006) **Expert Report: Telecommunications** [Internet] Available from <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf>. [Accessed 20 December 2006].

Greene, Thomas (2001) **Face recognition useless for crowd surveillance** [Internet] Available from <http://www.theregister.co.uk/2001/09/27/face_recognition_useless_for_crowd/> [Accessed 10th May 2004]

Grossman, W. M. (2006) **Will logging your email combat terrorism in Europe?, Thursday January 12, 2006** [Internet] Available from <http://technology.guardian.co.uk/weekly/story/0,16376,1683944,00.html>. [Accessed 13 April 2006].

GSM Europe (2005) **Facts & Figures, Source: Wireless Intelligence (September 2005)**. [Internet] Available from:<http://www.gsmworld.com/gsmeurope/news/facts.shtml> [Accessed 15 April 2006]

Haig, B. D. (1995) **Grounded Theory as Scientific Method**, Philosophy of Education Society [Internet] Available from <http://www.psyencelab.com/documents/Haig%20Grounded%20Theory%20as%20Scientific%20Method.pdf>. [Accessed 14 August 2006].

Harkin, J. (2003) **Mobilisation: the growing public interest in mobile technology**, Demos, London.

HL 51, HC 420 (2001-02) **Joint Committee on Human Rights, Anti-terrorism, Crime and Security Bill: Further Report, , Appendices to the Minutes of Evidence, Appendix 1: Comments of the Information Commissioner, para. 2.** [Internet] Available from: <http://www.publications.parliament.uk/pa/jt200102/jtselect/jtrights/51/51ap02.htm> [Accessed 10 July 2007]

HL38, HC 381 (2003-04) **HC/HL Joint Committee on Human Rights, Sixth Report on Anti-terrorism, Crime and Security Act 2001: Statutory Review and Continuance of Part 4, HL38/HC 381, 24 February, 2004**. [Internet] Available from:<http://www.publications.parliament.uk/pa/jt200304/jtselect/jtrights/38/3804.htm#a1> [Accessed 10 July 2007]

HL Debate (2001) **Daily Hansard, Volume No. 629, Part No. 53, col. 189, November 27, 2001 (Lord Waddington).** [Internet] Available from:<http://www.publications.parliament.uk/pa/ld200102/ldhansrd/vo011127/text/11127-08.htm#11127-08_head0> [Accessed 11 July 2007]

Home Office (1999) **Interception of Communications in the United Kingdom**. [Internet] Available from:<http://www.homeoffice.gov.uk/documents/cons-1999-interception-comms?view=Binary> [Accessed 07 July 2007]

Home Office (2003a) **Access to Communications Data - Respecting Privacy and Protecting the Public from Crime - a consultation paper**. [Internet] Available from:<http://www.homeoffice.gov.uk/documents/consult.pdf?view=Binary> [Accessed 23 February 2004]

Home Office (2003b) **Consultation Paper on a code of practice for voluntary retention of communications data**. [Internet] Available from:<http://www.homeoffice.gov.uk/docs/vol_retention.pdf> [Accessed 17 July 2004]

Home Office (2003c) **Retention of Communications data under Part 11: Anti-Terrorism, Crime & Security Act 2001 - Voluntary Code of Practice**. [Internet] Available from:<http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> [Accessed 06 August 2006]

Home Office (2006) **Acquisition and Disclosure of Communications Data, Revised Draft Code of Practice - A public consultation**. [Internet] Available from:<http://www.homeoffice.gov.uk/documents/351628/ripa-part1.pdf?view=Binary> [Accessed 03 August 2006]

Hosein, I., Whitley, E. (2002) **The regulation of electronic commerce : learning from the UK's RIP Act** Journal of strategic information systems, 11 (1). pp. 31-58. [Internet] Available from <http://eprints.lse.ac.uk/archive/00000271/01/Hosein_JSIS_paper.pdf> [Accessed 07 August 2006]

Hosein, I., Escudero-Pascual, A. (2002) Understanding Traffic Data and Deconstructing Technology-neutral Regulations [Internet] Available from <http://www.it.kth.se/~aep/publications/unece-latest-escuderoa-hoseini.pdf>. [Accessed 23 August 2004].

Hosein, G. (Ed.) (2003) **Privacy, Technology, and Europe - A Report for Japan's Ministry of Public Management Home Affairs Postal and Telecommunications**.

Hosein, I. (2004) The Sources of Laws: Policy dynamics in a Digital and Terrorized World. **The Information Society***,* Vol. 20, 187-199.

Hosein, G. (2005a) **Essays for civil liberties and democracy in Europe - What's wrong with Europe?** [Internet] Available from:<http://www.ecln.org/essays/essay-15.pdf> [Accessed 16 December 2005]

Hosein, G. (2005b) **Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe, December 13, 2005** [Internet] Available from <http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf> [Accessed 01 August 2006]

House of Commons Debate (2000) [Internet] Available from:<http://www.publications.parliament.uk/pa/cm199900/cmhansrd/vo000306/debtext/00306-06.htm> [Accessed 04 July 2007]

Hubaux, J., Znaty, S. (2000) In: Terplan, K., Morreale, P., ed. **The Telecommunications Handbook**. CRC Press LLC.

Human Rights Act 1998 (c. 42) HMSO, London.

Hunter, R. (2002) **World Without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing***,* John Wiley & Sons, Inc.

Independent Expert Group on Mobile Phones (2000) **Mobile Phones and Health**. [Internet] Available from:<http://www.iegmp.org.uk/report/text.htm> [Accessed 09 December 2006]

Information Commissioner's Office (n.d.) **Website - What we cover** [Internet] Available from <http://www.ico.gov.uk/>. [Accessed 23 January 2007].

Information Commissioner (2007) **Inquiry into 'The Surveillance Society?' - Evidence Submitted by the Information Commissioner**. [Internet] Available from:<http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/home_affairs_committee_inquiry_into_surveillance_society.pdf> [Accessed 15 July 2007]

International Chamber of Commerce (2002) **Policy Statement - Storage of traffic data for law enforcement purposes, prepared by the Commission on E-Business, IT and Telecoms** [Internet] Available from <http://www.iccwbo.org/home/news_archives/2002/stories/traffic%20data.pdf> [Accessed 04 August 2006]

International Telecommunication Union (2003) **ITU Glossary of Mobile Internet Terms**. [Internet] Available from:<http://www.itu.int/osg/spu/imt-2000/SPU%20Mobile%20Glossary%202003.pdf> [Accessed 15 April 2005]

Introna, L. (1997) Privacy and the Computer: Why we need Privacy in the Information Society. **Metaphilosophy 28 (3), 259–275**.

Johnson, D. G. (2001) **Computer ethics***,* Prentice-Hall, Inc., Upper Saddle River.
Kalakota, R., Robinson, M. (2001) **e-Business 2.0 - Roadmap for Success***,* Addison-Wesley, New York.

Kaupins, G., Minch, R. (2005) **Legal and Ethical Implications of Employee Location Monitoring**. [Internet] Available from:<http://csdl2.computer.org/comp/proceedings/hicss/2005/2268/05/22680133a.pdf> [Accessed 01 November 2005]
Kim, M. (2004) Surveillance Technology, Privacy and Social Control. **International Sociology***,* Vol. 19, No. 2, 193-213.

Langford, D. (2000) **Internet Ethics***,* Macmillan Press Ltd, London.

Leeds Metropolitan University (2006) **Policy, Framework Principles & Procedures for Research Ethics.** [Internet] Available from <http://www.leedsmet.ac.uk/research/PublishedPolicyFramework(res_Ethics).doc> [Accessed 02 November 2006]

Leyden, J. (2005) MEPs vote for mandatory data retention. **The Register**, [Internet] Available from <http://www.theregister.co.uk/2005/12/14/eu_data_retention_vote/> [Accessed 31 July 2006]

Liberty (The National Council for Civil Liberties) (Ed.) (1999) **Liberating cyberspace: Civil liberties, Human rights, and the Internet**, London, Pluto Press in association with Liberty.

Liberty (2003) **Liberty response to the Home Office consultation: 'A Code of Practice for Voluntary Retention of Communications Data', June 2003** [Internet] Available from <http://www.liberty-human-rights.org.uk/resources/policy-papers/policy-papers-2003/pdf-documents/vol-retention-of-comms-data.pdf> [Accessed 02 August 2006]

Liberty (n.d.) **CLOSED CIRCUIT TELEVISION - CCTV**. [Internet] Available from:<http://www.liberty-human-rights.org.uk/privacy/cctv.shtml> [Accessed 05 March 2006]

Lloyd, I. J. (2004) **Information technology law**. 4th ed. Oxford University Press, Oxford.

Louis Harris & Associates Inc. and Westin, A. F. (1979) **The dimensions of privacy: a National Opinion Research Survey of attitudes towards privacy**. Sentry Insurance, Stevens Point, Wisconsin.

Lyon, D. (1994) **The electronic eye : the rise of surveillance society**, Polity Press, Oxford.

Lyon, D. (2001) **Surveillance Society - Monitoring everyday life**, Open University Press, Buckingham

Lyon, D. (2002) Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. **Surveillance & Society***.* Volume 1(1): pages 1-7.

Lyon, D. (Ed.) (2003) **Surveillance as Social Sorting - Privacy, Risk and Digital Discrimination***,* Routledge, London.

Lyon, D., Marmura, S., Peroff, P. (2005) **Location Technologies: Mobility, Surveillance and Privacy - Report to the Office of the Privacy Commissioner of Canada. March 2005** [Internet] Available from <http://www.queensu.ca/sociology/Surveillance/files/loctech.pdf> [Accessed 03 January 2005]

m-Location (n.d.) **Mobile Locatin Based Services (LBS)** [Internet] Available from <http://www.m-location.com/html/MobileLocationBasedServices.htm>. [Accessed 03 September 2004].

Marshall, C.; Rossman, G. (1999) **Designing Qualitative Research**. 3rd ed. Thousand Oaks, Ca., Sage.

Martin, E. A. (2003) **A dictionary of law**. 5th ed. Oxford University Press, Oxford.

Marx, G. T. (2001) Murky conceptual waters: the public and the private. **Ethics and Information Technology***,* Vol. 3, no.3, pp. 157-169.

Marx, G. T. (2002) What's New About the "New Surveillance"? Classifying for Change and Continuity. **Surveillance & Society***,* Vol. 1, issue 1, pp. 9-29.

Marx, G. T. (2006) **Rocky Bottoms and Some Information Age Techno-Fallacies** [Internet] Available from <http://web.mit.edu/gtmarx/www/rockybottoms.html>. [Accessed 23 March 2007].

Mason, R. (1986) Four Ethical Issues of the Information Age. **Management Information Systems Quarterly***,* March 1986, vol.10, no.1, pp. 5-12.

Mason, R. (n.d.) **A tapestry of privacy**. [Internet] Available from <http://cyberethics.cbi.masstate.edu/mason2/> [Accessed 20th March 2004]

Mast Sanity (2006) **Mast Sanity website**. [Internet] Available from:<http://www.mastsanity.org/> [Accessed 18 December 2006]

Mathieson, S. (2001) **You can ring, but you can't hide** [Internet] Available from <www.guardian.co.uk>. [Accessed 16th March 2004].

Mathieson, S. (2003) Keeping 1984 in the past. **The Guardian**, June 19, 2003.

Mathieson, S. (2004) Eyes on the child. **The Guardian**, 29th January 2004.

May, C. (2002) **The information society : a sceptical view***,* Polity Press, Cambridge.

McAuliffe, W. (2001) **European Parliament restricts access to personal data**. [Internet] Available from:<http://news.zdnet.co.uk/emergingtech/0,1000000183,2091211,00.htm> [Accessed 01 August 207]

McKinlay, A., Starkey, K. (Ed.) (1998) **Foucult, Management and Organization Theory - From Panopticon to Technologies of Self**, Sage Publications.

McLuhan, M. (1964) **Understanding media: The extensions of man**. London, Routeledge and Kegan Paul.

Miles, M., Huberman, A. (1994) **An Expanded Sourcebook - Qualitative Data Analysis, 2nd ed.** Thousand Oaks, California, SAGE Publications, Inc.

Millar, S., Kelso, P. (2001) **Liberties fear over mobile phone details**. [Internet] Available from:<http://www.guardian.co.uk/mobile/article/0,2763,581763,00.html> [Accessed 10 August 2007]
Mobile Operators Association (2006) **The need for mobile networks**. [Internet] Available from: <http://www.mobilemastinfo.com/information/fact_sheets/need_for_mobile_networks.htm> [Accessed 15 November 2006]
Moran, M. (2005) **Politics and Governance in the UK**. Palgrave Macmillan, Hampshire.

Mill, J. (1974) **On Liberty**. Prometheus Books, Loughton.

Mobile Operators Association (MOA) (2006) **History of cellular mobile communications**. [Internet] Available from:<http://www.mobilemastinfo.com/information/history.htm> [Accessed 15 November 2006]

Monmonier, Mark (2002) **Spying with maps**. Chicago, The University of Chicago Press, Ltd.

Moore, C. (2006) **Market for mobile LBS to reach €622m by 2010**. [Internet] Available from:<http://www.dmeurope.com/default.asp?ArticleID=18318> [Accessed 19 September 2006]

Munir, A. (2005) **Retention of Communications Data: Security vs Privacy, Safety & Security in a Networked World - an oxford internet institute conference** [Internet] Available from <http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers> [Accessed 04 July 2006]

National Radiological Protection Board (2004) **Mobile Phones and Health 2004, Report by the board of NRPB**. [Internet] Available from:<http://www.hpa.org.uk/radiation/publications/documents_of_nrpb/pdfs/doc_15_5.pdf> [Accessed 09 December 2006]

National Statistics (2005) **Society, Consumer Durables** [Internet] Available from:<http://www.statistics.gov.uk/CCI/nugget.asp?ID=868&Pos=4&ColRank=2&Rank=448> [Accessed 15 November 2006]

National Statistics (2006) **Population Estimates**. [Internet] Available from:<http://www.statistics.gov.uk/CCI/nugget.asp?ID=6> [Accessed 15 November 2006]

Nissenbaum (1998) Protecting Privacy in an Information Age: The Problem of Privacy in Public. **Law and Philosophy**, 17: 559-596.

Ofcom (2006) **The Communications Market 2006** [Internet] Available from <http://www.ofcom.org.uk/research/cm/cm06/> [Accessed 22 September 2006].

Office of Surveillance Commissioners (2003) **Website - How we work** [Internet] Available from <http://www.surveillancecommissioners.gov.uk>. [Accessed 23 January 2007].

Open Letter from civil society groups (2005) **Open Letter from civil society groups to the European Parliament calling on MEPs to reject Data Retention, 06 December 2005** [Internet] Available from <http://www.statewatch.org/news/2005/dec/ep-let-dat-ret.htm> [Accessed 09 February 2006]

Orwell, G. (1959) **Nineteen eighty-four: a novel***,* Secker & Warburg, London.

Parliamentary Office of Science and Technology (2002) **postnote - Electronic Privacy, October 2002, Number 183**. [Internet] Available from:<http://www.parliament.uk/post/pn183.pdf> [Accessed 14th December 2003]

Prasad, M. (n.d.) **Location based services** GIS Development [Internet] Available from <http://www.gisdevelopment.net/technology/lbs/techlbs003pf.htm> [Accessed 24 April 2006]

Privacy International (2002) **An international survey of privacy laws and developments**. Electronic Privacy Information Center (USA) and Privacy International (UK) [Internet] Available from <http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf>. [Accessed 20 January 2006].

Privacy International (2003a) **Data Retention violates human rights convention**. [Internet] Available from: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-57875> [Accessed 06 August 2006]

Privacy International (2003b) **An international survey of privacy laws and developments.** [Internet] Available from <http://www.privacyinternational.org> [Accessed 16th December 2003]

Privacy International (2003c) **Memorandum oflaws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights**. [Internet] Available from:<http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf> [Accessed 11 November 2006]

Privacy International (2004) **Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention. September 2004** [Internet] Available from <http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html> [Accessed 12 December 2004]

Questionnaire on traffic data retention- 11490/1/02 REV 1 (2002) [Internet] Available from <http://www.statewatch.org/news/2002/aug/11490-r1.pdf>. [Accessed 15 June 2006].

Questionnaire on traffic data retention 10767/04 (2004) [Internet] Available from <http://register.consilium.eu.int/pdf/en/04/st10/st10767.en04.pdf>. [Accessed 16 June 2006].

Raab, C., Bennett, C. (2006) **The Governance of Privacy: Policy Instruments in Global Perspective**. The MIT Press, Cambridge.

Reed, C., Angel, J. (Ed.) (2007) **Computer law : the law and regulation of information technology**, Oxford University Press, Oxford.

Regulation of Investigatory Powers Act 2000 [Internet] Available from <http://www.opsi.gov.uk/acts/acts2000/20000023.htm> [Accessed 29 July 2006]

Responses to the data retention questionnaire (2002) [Internet] Available from <http://servizi.radicalparty.org/data_retention/>. [Accessed 15 June 2006].

Reporters without borders (2004) **United Kingdom** [Internet] Available from <http://www.rsf.org/article.php3?id_article=10686> [Accessed 08th July 2004]

Robson, C. (2002) **Real world research : a resource for social scientists and practitioner-researchers**. 2nd ed. Oxford, Blackwell Publishers Ltd.

Select Committee on Home Affairs (2001) **First Report - THE ANTI-TERRORISM, CRIME AND SECURITY BILL** [Internet] Available from <http://www.publications.parliament.uk/pa/cm200102/cmselect/cmhaff/351/35104.htm#a2> [Accessed 29 July 2006]

Shah, S. (2005) THE UK'S ANTI-TERROR LEGISLATION AND THE HOUSE OF LORDS: THE FIRST SKIRMISH. **Human Rights Law Review**, Vol. 5, pp. 403-421.

Sherriff, L. (2005) Music biz to 'hijack' Europe's data retention laws - from terrorism to filesharing. **The Register**, 25th November 2005. [Internet] Available from <http://www.theregister.co.uk/2005/11/25/data_retention/> [Accessed 27 November 2005]

Singh, T., Hill, M. (2003) Consumer privacy and the Internet in Europe: a view from Germany. **Journal of consumer marketing**, Vol. 20 No. 7, pp.634-651.

SnapTrack- A QUALCOMM Company (2003) **Location Technologies for GSM, GPRS and UMTS Networks**. [Internet] Available from:<http://www.cdmatech.com/download_library/pdf/location_tech_wp_1-03.pdf> [Accessed 15 April 2006]

Solove, D. (2002) **Conceptualizing Privacy, California Law Review, Vol. 90, p. 1087** [Internet] Available from <http://papers/ssm.com/sol3/papers.cfm?abstract_id=313103> [Accessed 08 January 2006]

Spiekermann, S. (2004) **General Aspects of Location-Based Services** [Internet] Available from <http://amor.rz.hu-berlin.de/~spiekers/LBS_9286-Schiller-01.pdf> [Accessed 14 April 2006]

Spinney, J. (2004) **Location-Based Services and the Proverbial Privacy Issue** [Internet] Available from <http://www.locationintelligence.net/articles/510.html>. [Accessed 16th May 2004].

Stalder, F. (2002) Privacy is not the antidote to surveillance. **Surveillance & Society**, Vol. 1, issue 1, pp. 120-124.

Stallings, W. (2005) **Wireless Communications and Networks**. 2nd ed., New Jersey, Pearson Prentice Hall.

Statewatch News (2001a) **United States Mission to the European Union: Proposals for US-EU counter-terrorism cooperation**. [Internet] Available from:<http://www.statewatch.org/news/2001/nov/06Ausalet.htm> [Accessed 29 July 2006]

Statewatch News (2001b) **EU governments to give law enforcement agencies access to all communications data**. [Internet] Available from:<http://www.statewatch.org/news/2001/may/03Benfopol.htm> [Accessed 07 August 2007]
Statewatch (2001c) **G8 Conference on High-Tec Crime, 22-24 May 2001, Tokyo** [Internet] Available from <http://www.statewatch.org/news/2001/may/03Fenfopol.htm>. [Accessed 14 August 2007].

Statewatch News (2003) **UK: Data retention and access consultation farce - Government to allow access for crime purposes to records which can only be held for "national security"** september 2003 [Internet] Available from <http://www.statewatch.org/news/2003/sep/11Batcs.htm> [Accessed 05 August 2006]

Statewatch News (2005a) **Data Retention: ALDE rapporteur considers Council proposal "disproportionate, invasive and illusory",** 04 May 2005. [Internet] Available from <http://www.statewatch.org/news/2005/may/eu-alde-data-retentoin.pdf> [Accessed 15 June 2005]

Statewatch News (2005b) **EU: Data Retention proposal partly illegal, say Council and commission lawyers** [Internet] Available from http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm [Accessed 14 July 2005]

Statewatch News, July 2005 (2005c) **UK-EU: Call for mandatory data retention of all telecommunications,** [Internet] Available from <http://www.statewatch.org/news/2005/jul/05eu-data-retention.htm> [Accessed 31 July 2006]

Steele, R., Hanzo, L., ed. (1999) **Mobile radio communications : second and third-generation cellular and WATM systems**. 2nd ed., Chichester, Wiley.

Steele, R., Lee, Ch., Gould, P. (2001) **GSM, cdmaOne and 3G Systems**. John Wiley and Sons, Ltd., Chichester, England.

Steiniger, S., Neun, M., Edwardes, A. (2006) **Foundations of Location Based Services, Lecture notes**. [Internet] Available from:<http://www.geo.unizh.ch/publications/cartouche/lbs_lecturenotes_steinigeretal2006.pdf> [Accessed 09 December 2006]
Stern, P. (1994) Eroding Grounded Theory. In: Morse, J. ed. **Critical Issues in Qualitative Research Methods**. Sage, Thousand Oaks, Ca.

STOA report - An appraisal of technologies for political control (1998) **European Parliament, Scientific and technological options assessmnet**. [Internet] Available from:<http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm> [Accessed 05 December 2003]

Stone, R. (2004) **Textbook on civil liberties and human rights**. 5th ed. Oxford, Oxford University Press.

Storey, T., Turner, C. (Ed.) (2005) **Unlocking EU Law***,* Hodder Arnold.

Strauss, A., Corbin, J. (1998) **Basics of Qualitative Research - Techniques and Procedures for Developing Grounded Theory**. London, Sage.

Surveillance Studies Network (2006) **A Report on the Surveillance Society**. [Internet] Available from: <http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx> [Accessed 15th November 2006]

Swinton, T. (2007) **Report of the Interception of Communications Commissioner for 2005-2006, Commissioner: THE RT HON SIR SWINTON THOMAS,** [Internet] Available from <http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf>. [Accessed 05 March 2007].

Taylor, N. (2002) State Surveillance and the Right to Privacy. **Surveillance & Society***,* Vol 1 (1), pp. 66 - 68.

Terrorism Act 2000 (chapter 11) London, HMSO. [Internet] Available from: <http://www.opsi.gov.uk/Acts/acts2000/20000011.htm> [Accessed 15th January 2007].

The Investigatory Powers Tribunal (2005) **Communications Data, 31 May 2005**. [Internet] Available from:<http://www.ipt-uk.com/default.asp?sectionID=1&chapter=1.5> [Accessed 03 August 2006]

The concise Oxford English dictionary. (2001) 10th ed. Oxford, Oxford University Press.

The Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002 (2002) [Internet] Available from <http://www.opsi.gov.uk/si/si2002/draft/ukdsi_0110423224_en.pdf#xml=http://www.hmso.gov.uk/cgi-bin/pdf_hl.pl?STEMMER=en&RGB=ff00ff&WORDS=regulation+investigatory+powers+commun+addit+public+author+&PAGE=1&DB=opsi&URL=http://www.opsi.gov.uk/si/si2002/draft/ukdsi_0110423224_en.pdf> [Accessed 05 August 2006]

Thompson, B. (2005) Fight for your right to privacy. **BBC News**, 25 November 2005. [Internet] Available from <http://news.bbc.co.uk/1/hi/technology/4469886.stm> [Accessed 27 November 2005]

Tomkins, A. (2002) 'Legislating Against the Terror: the Anti-Terrorism, Crime and Security Act 2001'. **Public Law***,* pp. 205-220.

UK Parliament (2001) **Explanatory Notes to Anti-Terrorism, Crime and Security Act 2001** [Internet] Available from <http://www.opsi.gov.uk/acts/en2001/2001en24.htm> [Accessed 29 July 2006]

UK Presidency of European Union (2005) **Liberty and security, striking the right balance** [Internet] Available from <http://www.statewatch.org/news/2005/sep/ukpres-paper.pdf> [Accessed 02 August 2006]

UMTS Forum **What is UMTS ?** [Internet] Available from:<http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/What+is+UMTS_index> [Accessed 18 April 2006]

US Patent full-text and image database (1972) **United States Patent, MOBILE COMMUNICATION SYSTEM, May 16, 1972**. [Internet] Available from:<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=3663762.PN.&OS=PN/3663762&RS=PN/3663762> [Accessed 19 December 2006]

Van Riper, D., Whitfield, T. (2004) **P6 – Rough Draft of Project Report: Developing a Framework for Privacy in Location-Based Services**. [Internet] Available from:<http://www.socsci.umn.edu/~tomw/csci8715/p6.pdf> [Accessed 15 November 2006]

Varshney, U. (2003) **Location Management for Mobile Commerce Applications in Wireless Internet Environment** [Internet] Available from <http://www.cis.gsu.edu/~uvarshne/papers/ToIT.pdf>. [Accessed 17 April 2005].

Vilasau, M. (2007) Traffic Data Retention v Data Protection: The new European framework. **Computer and Telecommunications Law Review***,* Vol. 13 (2), pp. 52-59.

Virgo, P., Rogers, B. (2003) **IT Managers support regulation of investigatory powers but not data retention** [Internet] Available from <http://www.fipr.org/sfs7/virgo.html> [Accessed 04 August 2006]

Viseu, A., Clement, A., Aspinall, J. (2004) Situating privacy online: Complex perceptions and everyday practices. **Information, Communication & Society***,* Vol. 7, No. 1 / March 2004**,** 15 November 2005.

Vodafone (2005) **Policy For Provision of Customer Location Data to Commercial Location Based Service Providers**. [Internet] Available from:<https://www.vodafonemobileideas.co.uk/vfthirdparty/process.do;jsessionid=05930C6ECF2021525E8B3CDF3C89A319?action=display&xml_content=public/wholesale/downloads/product/location_services/regulatory/location_services_policy.pdf> [Accessed 17 April 2006]

Vodafone (2006) **Mobile phone contract information** [Internet] Available from:< http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?_nfpb=true&_pageLabel=Page_BOS_MainContent&pageID=AV_0559> [Accessed 01 September 2006]

Wadham, J. (1999) No, you're turning us all into criminals. **The Guardian**, [Internet] Available from <http://www.guardian.co.uk/comment/story/0,,246679,00.html> [Accessed 07 August 2007].

Walke, B. H. (1999) **Mobile Radio Networks: Networking and Protocols**. Wiley, Chichester.

Walke, B., Seidenberg, P., Althoff, M. P. (2003) **UMTS: The Fundamentals**. John Wiley & Sons, Ltd., Chichester.

Walker, C., (2002) **Blackstone's Guide to the Anti-Terrorism Legislation**. Oxford University Press, Oxford.

Walker, C., Akdeniz, Y. (2003) **Anti-Terrorism Laws and Data Retention: War is over?** [Internet] Available from <http://www.cyber-rights.org/documents/data_retention_article.pdf> [Accessed 06 August 2006]

Walters, L., Kritzinger, P. (2000) **Cellular Networks: Past, Present, and Future (Crossroads - The ACM Student Magazine)** [Internet] Available from <http://www.acm.org/crossroads/xrds7-2/cellular.html> [Accessed 15 March 2006]

Ward, M. (2000) 'Snooping' bill protests stepped up. **BBC online news**, 12 July 2000 [Internet] Available from <http://news.bbc.co.uk/1/hi/sci/tech/830318.stms> [Accessed 29 July 2006]

Ward, M. (2001) Government 'snoop law' stance slammed. **BBC New Online**, 17 May 2001 [Internet] Available from <http://news.bbc.co.uk/1/hi/sci/tech/1335963.stm> [Accessed 29 July 2006]

Warren, P. (2006) Lifting the veil on internet voices. **The Guardian**, 27 July 2006 [Internet] Available from <http://technology.guardian.co.uk/weekly/story/0,,1830460,00.html> [Accessed 08 August 2006]

Warren, S., Brandeis, L. (1890) **The Right of Privacy**. Harvard Law Review 4 [Internet] Available from <http://www.Lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html> [Accessed 16th November, 2003]

Webster, F. (1995) Theories of the information society. Routledge, London.

Westin, A. F. (Ed.) (1971) **Information Technology in a Democracy***,* Harvard University Press, Cambridge.

Weitzman, E. A. (2000). **Software and qualitative research**. In N. K. Denzin & Y. S. Lincoln, (Eds.). Handbook of qualitative research*.* 2d edition. pp. 803-820.Thousand Oaks, CA: Sage.

Where-RU (2004) **Location Tracking Service** [Internet] Available from <http://www.where-ru.com/how.php> [Accessed 18th May 2004]

White, J. C. (2003) **People, Not Places: A Policy Framework for Analyzing Location Privacy Issues (Masters Memo Prepared for the Electronic Privacy Information Center): Terry Sanford Institute of Public Policy, Duke University.** [Internet] Available from: <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf> [Accessed 27 November 2004]

Whitley, E., Hosein, I. (2005) **Policy discourse and data retention: The technology politics of surveillance in the United Kingdom** [Internet] Available from <http://personal.lse.ac.uk/whitley/allpubs/TPRetention.pdf>. [Accessed 15 May 2006].

Whitty, N., Murphy, T., Livingstone, S. (2001) **Civil liberties law : the human rights act era**. Butterworths, London.

Wood, D. (2001) **The Hidden Geography of Transnational Surveillance: Social and technological networks around signals intelligence sites** [Internet] Available from <http://www.staff.ncl.ac.uk/d.f.j.wood/thesis_webpreface.htm>. [Accessed 15 April 2005].

Woolgar, S. (Ed.) (2002) **Virtual society? : technology, cyberbole, reality***,* Oxford University Press, Oxford.

Zureik, E. (2004) **Overview of Public Opinion Research Regarding Privacy**. [Internet] Available from:<http://www.queensu.ca/sociology/Surveillance/research-sections.htm> [Accessed 06th May 2004].

Zureik, E., Salter, M. B. (Ed.) (2005) **Global Suveillance and Policing - Borders, security, identity***,* Willan Publishing, Cullompton and Oregon.