Roba Abbas, Katina Michael, M.G. Michael:

Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World

Abstract:

The idea for an Internet of Things has matured since its inception as a concept in 1999. People today speak openly of a Web of Things and People, and even more broadly of an Internet of Everything. As our relationships become more and more complex and enmeshed, through the use of advanced technologies, we have pondered on ways to simplify flows of communications, to collect meaningful data, and use them to make timely decisions with respect to optimisation and efficiency. At their core, these flows of communications are pathways to registers of interaction, and tell the intricate story of outputs at various units of analysis- things, vehicles, animals, people, organisations, industries, even governments. In this trend toward evidence-based enquiry, data is the enabling force driving the growth of IoT infrastructure. This paper uses the case of location-based services, which are integral to IoT approaches, to demonstrate that new technologies are complex in their effects on society. Fundamental to IoT is the spatial element, and through this capability, the tracking and monitoring of everything, from the smallest nut and bolt, to the largest shipping liner to the mapping of planet earth, and from the whereabouts of the minor to that of the prime minister. How this information is stored, who has access, and what they will do with it, is arguable depending on the stated answers. In this case study of location-based services we concentrate on control and trust, two overarching themes that have been very much neglected, and use the outcomes of this research to inform the development of a socio-ethical conceptual framework that can be applied to minimise the unintended negative consequences of advanced technologies. We posit it is not enough to claim objectivity through information ethics approaches alone, and present instead a socio-ethical impact framework. Sociality therefore binds together that higher ideal of praxis where the living thing (e.g. human) is the central and most valued actor of a system.

Agenda:

ISSN 1614-1687

Authors:

Honorary Fellow Dr Roba Abbas:

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 - 4221 - 3555 , ✉ roba@uow.edu.au 💻http://www.technologyandsociety.org/members/2013/7/25/dr-roba-abbas
- Relevant publications:
  - *R. Abbas, K. Michael, M.G. Michael, R. Nicholls, Sketching and validating the location-based services (LBS) regulatory framework in Australia, Computer Law and Security Review 29, No.5 (2013): 576-589.*
  - *R. Abbas, K. Michael, M.G. Michael, The Regulatory Considerations and Ethical Dilemmas of Location-Based Services (LBS): A Literature Review, Information Technology & People 27, No.1 (2014): 2-20.*

Associate Professor Katina Michael:

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 - 4221 - 3937 , ✉ katina@uow.edu.au 💻 http://ro.uow.edu.au/kmichael
- Relevant publications:
  - *K. Michael, R. Clarke, Location and Tracking of Mobile Devices: Überveillance Stalks the Streets, Computer Law and Security Review 29, No.3 (2013): 216-228.*
  - *K. Michael, M. G. Michael, Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants, IGI Global, (2009).*
  - *L. Perusco, K. Michael, Control, trust, privacy, and security: evaluating location-based services, IEEE Technology and Society Magazine 26, No.1 (2007): 4-16.*

Honorary Associate Professor M.G. Michael

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 – 4221 - 3937, ✉ mgm@uow.edu.au, 💻 http://ro.uow.edu.au/mgmichael
- Relevant publications:
  - *M.G. Michael and K. Michael (eds) Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies, Hershey: PA, IGI Global, (2013).*
  - *K. Michael, M. G. Michael, "The Social and Behavioral Implications of Location-Based Services, Journal of Location-Based Services, Volume 5, Issue 3-4, (2011), 121-137.*
  - *M.G. Michael, K. Michael, Towards a State of Uberveillance, IEEE Technology and Society Magazine, 29, No.2, (2010): 9-16.*
  - *M. G. Michael, S. J. Fusco, K. Michael, A Research Note on Ethics in the Emerging Age of Uberveillance, Computer Communications, 31 No.6, 2008: 1192-1199.*

Introduction

Locative technologies are a key component of the Internet of Things (IoT). Some scholars go so far as to say it is the single most important component that enables the monitoring and tracking of subjects and objects. Knowing where something or someone is, is of greater importance than knowing who they are because *it* or *they* can be found, independent of *what* or *who* they are. Location also grants us that unique position on the earth's surface, providing for us one of the vital pieces of information forming the distance, speed, time matrix. A unique ID, formed around an IP address in an IoT world, presents us with the capability to label every living and non-living thing and to recollect it, adding to its history and longer term physical lifetime. But without knowing where something is, even if we have the knowledge that an action is required toward some level of maintenance, we cannot be responsive. Since the introduction of electronic databases, providing accurate records for transaction processing has been a primary aim. Today, however, we are attempting to increase visibility using high resolution geographic details, we are contextualizing events through discrete and sometimes continuous sensor-based rich audio-visual data collection, and we are observing how mobile subjects and objects interact with the built environment. We are no longer satisfied with an approach that says *identify all things*, but we wish to be able to recollect or activate them on demand, understand associations and affiliations, creating a digital chronicle of its history to provide insights toward sustainability.

There is thus an undue pressure on the ethical justification for social and behavioral tracking of people and things in everyday life. Solely because we have the means to do something, it does not mean we should do it. We are told that through this new knowledge gained from big data we can reduce carbon emissions, we can eradicate poverty, we can grant all people equity in health services, we can better provision for expected food shortages, utilize energy resources optimally, in short, make the world a better place. This utopian view might well be the vision that the tech sector wish to adopt as an honourable marketing strategy, but the reality of thousands of years of history tells us that technology does not necessarily on its own accord, make things better. In fact, it has often made some aspects of life, such as conflict and war, much worse through the use of modern, sophisticated advanced techniques. We could argue that IoT will allow for care-based surveillance that will bring about aid to individuals and families given needs, but the reality is that wherever people are concerned, technology may be exploited towards a means for control. Control on its own is not necessarily an evil, it all depends on how the functionality of given technologies are applied. Applied negatively the recipient of this control orientation learns distrust instead of trust which then causes a chain reaction throughout society, especially with respect to privacy and security. We need only look at the techniques espoused by some governments in the last 200 years to acknowledge that heinous crimes against humanity (e.g. democide) have been committed with new technological armaments (Rummel, 1997) to the detriment of the citizenry.

A socio-ethical framework is proposed as a starting point for seeking to understand the social implications of location services, applicable to current and future applications within IoT infrastructure. To stop at critiquing services using solely an information ethics-based approach is to fall short. Today's converging services and systems require a greater scope of orientation to ask more generally how society may be affected at large, not just whether information is being collected, stored, and shared appropriately. To ask questions about how location services and IoT technology will directly and indirectly change society has far greater importance for the longer term vision of person-to-person and person-to-thing interactions than simply studying various attributes in a given register.

Studies addressing the social implications of emerging technologies, such as LBS, generally reflect on the risks and ethical dilemmas resulting from the implementation of a particular technology within a given social context. While numerous approaches to ethics exist, all are inextricably linked to ideas of morality, and an ability to distinguish good conduct from bad. Ethics, in simple terms, can be considered as the "study of morality" (Quinn 2006, p. 55), where morality refers to a "system of rules for guiding human conduct and principles for evaluating those rules" (Tavani 2007, p. 32). This definition is shared by Elliot and Phillips (2004, p. 465), who regard ethics as "a set of rules, or a decision procedure, or both, intended to provide the conditions under which the greatest number of human beings can succeed in 'flourishing', where 'flourishing' is defined as living a fully human life" (O'Connor and Godar 2003, p. 248).

According to the literature, there are two prominent ethical dilemmas that emerge with respect to locating a person or thing in an Internet of Things world. First, the risk of unauthorised disclosure of one's location which is a breach of privacy; and second the possibility of increased monitoring leading to unwarranted surveillance by institutions and individuals. The socio-ethical implications of LBS in the context of IoT can therefore be explored based on these two major factors. IoT more broadly, however, can be examined by studying numerous social and ethical dilemmas from differing perspectives. Michael et al. (2006a, pp. 1-10) propose a framework for considering the ethical challenges emerging from the use of GPS tracking and monitoring solutions in the control, convenience and care usability contexts. The authors examine these contexts in view of the four ethical dimensions of privacy, accuracy, property and accessibility (Michael et al. 2006a, pp. 4-5). Alternatively, Elliot and Phillips (2004, p. 463) discuss the social and ethical issues associated with m-commerce and wireless computing in view of the privacy and access, security and reliability challenges. The authors claim that factors such as trust and control are of great importance in the organisational context (Elliot and Phillips 2004, p. 470). Similar studies propose that the major themes regarding the social implications of LBS be summarised as control, trust, privacy and security (Perusco et al. 2006; Perusco and Michael 2007). These themes provide a conceptual framework for reviewing relevant literature in a structured fashion, given that a large number of studies are available in the respective areas.

This article, in the first instance, focusses on the control- and trust-related socio-ethical challenges arising from the deployment of LBS in the context of IoT, two themes that are yet to receive comprehensive coverage in the literature. This is followed by an examination of LBS in the context of the Internet of Things (IoT), and the ensuing ethical considerations. A socio-ethical framework is proposed as a valid starting point for addressing the social implications of LBS and delivering a conceptual framework that is applicable to current LBS use cases and future applications within an Internet of Things world.

Control

Control, according to the Oxford Dictionary (2012a), refers to the "the power to influence or direct people's behaviour or the course of events". With respect to LBS, this theme is examined in terms of a number of important concepts, notably surveillance, dataveillance, sousveillance and überveillance scholarship.

Surveillance

A prevailing notion in relation to control and LBS is the idea of exerting power over individuals through various forms of surveillance. Surveillance, according to sociologist David Lyon, "is the focused, systematic and routine attention to personal details for the purposes of influence, management, protection and or direction," although Lyon admits that there are exceptions to this general definition (Lyon 2007, p. 14). Surveillance has also been described as the process of methodically monitoring the behaviour, statements, associates, actions and/or communications of an individual or individuals, and is centred on information collection (Clarke 1997; Clarke 2005, p. 9).

The act of surveillance, according to Clarke (1988; 1997) can either take the form of personal surveillance of a specific individual or mass surveillance of groups of interest. Wigan and Clarke (2006, p. 392) also introduce the categories of object surveillance of a particular item and area surveillance of a physical enclosure. Additional means of expressing the characteristics of surveillance exist. For example, the phrase "surveillance schemes" has been used to describe the various surveillance initiatives available (Clarke 2007a, p. 28). Such schemes have been demonstrated through the use of a number of mini cases or vignettes, which include, but are not limited to, baby monitoring, acute health care, staff movement monitoring, vehicle monitoring, goods monitoring, freight interchange-point monitoring, monitoring of human-attached chips, monitoring of human-embedded chips, and continuous monitoring of chips (Clarke 2007c; Clarke 2007b, pp. 47-60). The vignettes are intended to aid in understanding the desirable and undesirable social impacts resulting from respective schemes.

Common surveillance metaphors

In examining the theme of control with respect to LBS, it is valuable to initially refer to general surveillance scholarship to aid in understanding the link between LBS and surveillance. Surveillance literature is somewhat dominated by the use of metaphors to express the phenomenon. A prevalent metaphor is that of the panopticon, first introduced by Jeremy Bentham (Bentham and Bowring 1843), and later examined by Michel Foucault (1977). Foucault's seminal piece *Discipline and Punish* traces the history of punishment, commencing with the torture of the body in the eighteenth century, through to more modern forms of punishment targeted at the soul (Foucault 1977). In particular, Foucault's account offers commentary on the notions of surveillance, control and power through his examination of Bentham's panopticon, which are pertinent in analysing surveillance in general and monitoring facilitated by LBS in particular. The panopticon, or "Inspection-House" (Bentham and Bowring 1843, p. 37), refers to Bentham's design for a prison based on the essential notion of "seeing without being seen" (p. 44). The architecture of the panopticon is as follows:

> *"The building is circular. The apartments of the prisoners occupy the circumference. You may call them, if you please, the cells... The apartment of the inspector occupies the centre; you may call it if you please the inspector's lodge. It will be convenient in most, if not in all cases, to have a vacant space or area all round, between such centre and such circumference. You may call it if you please the intermediate or annular area"* (Bentham and Bowring 1843, pp. 40-41).

Foucault (1977, p. 200) further illustrates the main features of the inspection-house, and their subsequent implications on constant visibility:

> *"By the effect of backlighting, one can observe from the tower ['lodge'], standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible...Full lighting and the eye of a supervisor ['inspector'] capture better than darkness, which ultimately protected. Visibility is a trap."*

While commonly conceived as ideal for the prison arrangement, the panopticon design is applicable and adaptable to a wide range of establishments, including but not limited to work sites, hospital, schools, and/or or any establishment in which individuals "are to be kept under inspection" (Bentham and Bowring 1843, p. 37). It has been suggested, however, that the panopticon functions as a tool for mass (as opposed to personal) surveillance in which large numbers of individuals are monitored, in an efficient sense, by a small number (Clarke 2005, p. 9). This differs from the more efficient, automated means of dataveillance (to be shortly examined). In enabling mass surveillance, the panopticon theoretically allows power to be. In examining the theme of control with respect to LBS, it is valuable to initially refer to general surveillance scholarship to aid in understanding the link between LBS and surveillance. Surveillance literature is somewhat dominated by the use of metaphors to express the phenomenon. Foucault (1977, pp. 202-203) provides a succinct summary of this point:

> *"He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."*

This self-disciplinary mechanism functions similarly, and can somewhat be paralleled, to various notions in George Orwell's classic novel *Nineteen Eighty Four* (Orwell 1949), also a common reference point in surveillance literature. *Nineteen Eighty Four* has been particularly influential in the surveillance realm, notably due to the use of "Big Brother" as a symbol of totalitarian, state-based surveillance. Big Brother's inescapable presence is reflected in the nature of surveillance activities. That is, that monitoring is constant and omnipresent and that "[n]othing was your own except the few cubic centimetres inside your skull" (Orwell 1949, p. 29). The oppressive authority figure of Big Brother possesses the ability to persistently monitor and control the lives of individuals, employing numerous mechanisms to exert power and control over his populace as a reminder of his unavoidable gaze.

One such mechanism is the use of telescreens as the technological solution enabling surveillance practices to be applied. The telescreens operate as a form of self-disciplinary tool by way of reinforcing the idea that citizens are under constant scrutiny (in a similar fashion to the inspector's lodge in the panopticon metaphor). The telescreens inevitably influence behaviours, enabling the state to maintain control over actions and thoughts, and to impose appropriate punishments in the case of an offence. This is demonstrated in the following excerpt:

> "It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away. A nervous tic, an unconscious look of anxiety, a habit of muttering to yourself – anything that carried with it the suggestion of abnormality, of having something to hide. In any case, to wear an improper expression on your face (to look incredulous when a victory was announced, for example) was itself a punishable offence" (Orwell 1949, p. 65).

The Internet of Things, with its ability to locate and determine *who* is or *what* is related to one another using a multiplicity of technologies, will enable authorities in power to infer what someone is likely to do in a given context. Past behavioural patterns, can for example, reveal a likely course of action with relatively no prediction required. IoT in all its glory will provide complete visibility- the question is what are the risks associated with providing that kind of capability to the state or private enterprise? In scenario analysis we can ponder how IoT in a given context will be used for good, how it will be used for bad, and a neutral case where it will have no effect whatsoever because the data stream will be ignored by the system owner. While IoT has been touted as the ultimate in providing great organisational operational returns, one can see how it can lend itself to location-based tracking and monitoring using a panopticon metaphor. Paper records and registers were used during World War 2 for the purposes of segregation, IoT and especially the ability to "locate on demand", may well be used for similar types of control purposes.

Applying surveillance metaphors to LBS

The aforementioned surveillance metaphors can be directly applied to the case of LBS within IoT. In the first instance, it can be perceived that the exploitation of emerging technologies, such as LBS, extends the notion of the panopticon in a manner that allows for inspection or surveillance to take place regardless of geographic boundaries or physical locations. When applying the idea of the panopticon to modern technologies, Lyon suggests that "Bentham's panopticon gives way to the electronic superpanopticon" (Lyon 2001, p. 108). With respect to LBS, this superpanopticon is not limited to and by the physical boundaries of a particular establishment, but is rather reliant on the nature and capabilities of the mobile devices used for 'inspection'. In an article titled "The Panopticon's Changing Geography", Dobson and Fischer (2007) also discuss progress and various manifestations of surveillance technology, specifically the panopticon, and the consequent implications on power relationships. From Bentham's architectural design, to the electronic panopticon depicted by Orwell, and contemporary forms of electronic surveillance including LBS and covert human tracking, Dobson and Fisher (2007, p. 308-311) claim that all forms of watching enable continuous surveillance either as part of their primary or secondary purpose. They compare four means of surveillance- analogue technologies as used by spies which have unlimited geographic coverage and are very expensive to own and operate, Bentham's original panopticon where the geographic view was internal to a building, George Orwell's big brother view which was bound by the extent of television cables, and finally human tracking systems which were limited only by the availability and granularity of cell phone towers.

A key factor in applying the panopticon metaphor to IoT is that individuals, through the use of mobile location devices and technologies, will be constantly aware of their visibility and will assume the knowledge that an 'inspector' may be monitoring their location and other available information remotely at any given time. Mobile location devices may similarly replace Orwell's idea of the telescreens as Big Brother's primary surveillance technology, resulting in a situation in which the user is aiding in the process of location data collection and thereby surveillance. This creates, as maintained by Andrejevic (2007, p. 95), a "widening 'digital enclosure' within which a variety of interactive devices that provide convenience and customization to users double as technologies for gathering information about them."

'Geoslavery'

Furthermore, in extreme situations, LBS may facilitate a new form of slavery, "geoslavery", which Dobson and Fischer (2003, pp. 47-48) reveal is "a practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave. Inherent in this concept is the potential for a master to routinely control time, location, speed, and direction for each and every movement of the slave or, indeed, of many slaves simultaneously." In their seminal work, the authors flag geoslavery as a fundamental human rights issue (Dobson and Fisher 2003, p. 49), one that has the potential to somewhat fulfil Orwell's Big Brother prophecy, differing only in relation to the sophistication of LBS in comparison to visual surveillance and also in terms of who is in control. While Orwell's focus is on the state, Dobson and Fischer (2003, p. 51) caution that geoslavery can also be performed by individuals "to control other individuals or groups of individuals."

From state-based to citizen level surveillance

Common in both *Discipline and Punish* and *Nineteen Eighty Four* is the perspective that surveillance activities are conducted at the higher level of the "establishment"; that is, institutional and/or state-based surveillance. However, it must be noted that similar notions can be applied at the consumer or citizen level. Mark Andrejevic (2007, p. 212), in his book *iSpy: Surveillance and Power in the Interactive Era*, terms this form of surveillance as "lateral or peer-to-peer surveillance." This form of surveillance is characterised by "increasing public access to the means of surveillance – not just by corporations and the state, but by individuals" (Andrejevic 2007, p. 212). Similarly, Barreras and Mathur (2007, pp. 176-177) state that wireless location tracking capabilities are no longer limited to law enforcement, but are open to any interested individual. Abbas et al. (2011, pp. 20-31) further the discussion by focussing on related notions, explicitly, the implications of covert LBS-based surveillance at the community level, where technologies typically associated with policing and law enforcement are increasingly available for use by members of the community. With further reference to LBS, Dobson and Fischer (2003, p. 51) claim that the technology empowers individuals to control other individuals or groups, while also facilitating extreme activities. For instance, child protection, partner tracking and employee monitoring can now take on extreme forms through the employment of LBS (Dobson and Fisher 2003, p. 49). According to Andrejevic (2007, p. 218), this "do-it-yourself" approach assigns the act of monitoring to citizens. In essence higher degrees of control are granted to individuals thereby encouraging their participation in the surveillance process (Andrejevic 2007, pp. 218-222). It is important to understand IoT in the context of this multifaceted "watching". IoT will not only be used by organisations and government agencies, but individuals in a community will also be granted access to information at small units of aggregated data. This has implications at a multiplicity of levels. Forces of control will be manifold.

Dataveillance

The same sentiments can be applied to the related, and to an extent superseding, notion of data surveillance, commonly referred to as *dataveillance*. Coined by Roger Clarke in the mid-eighties, dataveillance is defined as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1988). Clarke (2005, p. 9) maintains that this process is automated and therefore a relatively economical activity when compared with other forms of surveillance, in that dataveillance activities are centred on examination of the data trails of individuals. For example, traditional forms of surveillance rely on expensive visual monitoring techniques, whereas dataveillance is largely an economically efficient alternative (Clarke 1994; 2001d, p. 11). Visual behavioural monitoring (that is, traditional surveillance) is an issue, but is nonetheless overshadowed by the challenges associated with dataveillance, particularly with reference to personal and mass dataveillance (Clarke 2005, pp. 9-10). That is, *personal dataveillance* presents risks to the individual based primarily on the potential for the collected data/information to be incorrect or outdated, while *mass dataveillance* is risky in that it may generate suspicion amongst individuals (Albrecht & Michael, 2013).

Risks associated with dataveillance

Clarke's early and influential work on "Information Technology and Dataveillance" recognises that information technology is accelerating the growth of dataveillance, which presents numerous benefits and risks (Clarke 1988, pp. 498, 505-507). Clarke lists advantages in terms of safety and government applications, while noting the dangers associated with both personal and mass dataveillance (Clarke 1988, pp. 505-507). These risks can indeed be extended or applied to the use of location and tracking technologies to perform dataveillance activities, resulting in what can be referred to as "dataveillance on the move" (Michael and Michael 2012). The specific risks include: ability for behavioural patterns to be exposed and cross-matched, potentially for revelations that may be harmful from a political and personal perspective, rise in the use of "circumstantial evidence", transparency of behaviour resulting in the misuse of information relating to an individual's conduct, and "actual repression of the readily locatable and trackable individual" (Clarke 2001b, p. 219). Emerging from this analysis, and that concerning surveillance and related metaphors, is the significant matter of loss of control.

Loss of control

Michael et al. (2006a, p. 2) state, in the context of GPS tracking, that the issue of control is a leading ethical challenge given the invasive nature of this form of monitoring. The mode of control can differ depending on the context. For instance, the business context may include control through directing or 'pushing' advertisements to a specific individual, and at personal/individual level could signify control in the manner of "self-direction" (Perusco et al. 2006, p. 93). Other forms of social control can also be exercised by governments and organisations (Clarke 2003b), while emerging LBS solutions intended for the consumer sector extend the notion of control to community members (Abbas et al. 2011). This is an area that has not been adequately addressed in the literature. The subsequent risks to the individual are summarised in the following passage:

> *"Location technologies therefore provide, to parties that have access to the data, the power to make decisions about the entity subject to the surveillance, and hence exercise control over it. Where the entity is a person, it enables those parties to make determinations, and to take action, for or against that person's interests. These determinations and actions may be based on place(s) where the person is, or place(s) where the person has been, but also on place(s) where the person is not, or has not been"* (Wigan and Clarke 2006, p. 393).

Therefore GPS and other location devices and technologies may result in decreased levels of control from the perspective of the individual being monitored. For example, in an article based on the use of scenarios to represent the social implications associated with the implementation of LBS, Perusco and Michael (2007) demonstrate the various facets of control in relation to LBS. The discussion is generally centred on the loss of control which can be experienced in numerous ways, such as when a device does not accurately operate, or when an individual constantly monitors a family member in an attempt to care for them (Perusco and Michael 2007, pp. 6-7, 10). The authors raise valuable ideas with respect to control, such as the need to understand the purpose of control, the notion of consent, and developing methods to deal with location inaccuracies amongst others (p. 14). Perusco and Michael further assert that control has a flow-on effect on other issues, such as trust for instance, with the authors questioning whether it is viable to control individuals given the likely risk that trust may be relinquished in the process (p. 13).

Concurrent with loss of control, the issue of pre-emptive control with respect to LBS is a delicate one, specifically in relation to suspected criminals or offenders. Perusco et al. (2006, p. 92) state that the punishment of a crime is typically proportionate to the committed offence, thus the notion of pre-emptive monitoring can be considered fundamentally flawed given that individuals are being punished without having committed an offence. Rather, they are suspected of being a threat. According to Clarke and Wigan (2011), a person is perceived a threat, based on their "personal associations" which can be determined using location and tracking technologies to establish the individual's location in relation to others, and thus control them based on such details. This is where IoT fundamentally comes into play. While location information can tell us much about where an individual is at any point in time, it is IoT that will reveal the inter-relationships and frequency of interaction, and specific application of measurable transactions. IoT is that layer that will bring things to be scrutinized in new ways.

This calls for an evaluation of LBS solutions that can be used for covert operations. Covert monitoring using LBS is often considered a useful technique, one that promotes less opposition than overt forms of monitoring, as summarised below:

> *"Powerful economic and political interests are seeking to employ location and tracking technologies surreptitiously, to some degree because their effectiveness is greater that way, but mostly in order to pre-empt opposition"* (Clarke 2001b, p. 221).

Covert applications of LBS are increasingly available for the monitoring and tracking of social relations such as a partner or a child (Abbas et al. 2011). Regardless of whether covert or overt, using LBS for monitoring is essentially about control, irrespective of whether the act of controlling is motivated by necessity, or for more practical or supportive purposes (Perusco et al. 2006, p. 93).

Studies focussing on user requirements for control

The control dimension is also significant in studies focussing on LBS users, namely, literature concerned with user-centric design, and user adoption and acceptance of LBS and related mobile solutions. In a paper focussing on understanding user requirements for the development of LBS, Bauer et al. (2005, p. 216) report on a user's "fear" of losing control while interacting with mobile applications and LBS that may infringe on their personal life. The authors perceive loss of control to be a security concern requiring attention, and suggest that developers attempt to relieve the apprehension associated with increased levels of personalisation though ensuring that adequate levels of control are retained (Bauer et al. 2005, p. 216). This is somewhat supported by the research of Xu and Teo (2004, pp. 793-803), in which the authors suggest that there exists a relationship between control, privacy and intention to use LBS. That is, a loss of control results in a privacy breach, which in turn impacts on a user's intention to embrace LBS.

The aforementioned studies, however, fail to explicitly incorporate the concept of value into their analyses. Due to the lack of literature discussing the three themes of privacy, value and control, Renegar et al. (2008, pp. 1-2) present the privacy-value-control (PVC) trichotomy as a paradigm beneficial for measuring user acceptance and adoption of mobile technologies. This paradigm stipulates the need to achieve harmony amongst the concepts of privacy, value and control in order for a technology to be adopted and accepted by the consumer. However, the authors note that perceptions of privacy, value and control are dependent on a number of factors or entities, including the individual, the technology and the service provider (Renegar et al. 2008, p. 9). Consequently, the outcomes of Renegar et al.'s study state that privacy does not obstruct the process of adoption but rather the latter must take into account the value proposition in addition to the amount of control granted.

Monitoring using LBS: control versus care?

The focus of the preceding sections has been on the loss of control, the dangers of pre-emptive control, covert monitoring, and user perspectives relating to the control dimension. However, this analysis should not be restricted to the negative implications arising from the use of LBS, but rather should incorporate both the control and care applications of LBS. For instance, while discussions of surveillance and the term in general typically invoke sinister images, numerous authors warn against assuming this subjective viewpoint. Surveillance should not be considered in itself as disagreeable. Rather, "[t]he problem has been the presumptiveness of its proponents, the lack of rational evaluation, and the exaggerations and excesses that have been permitted" (Clarke 2007a, p. 42). This viewpoint is reinforced in the work of Elliot and Phillips (2004, p. 474), and can also be applied to dataveillance.

The perspective that surveillance inevitability results in negative consequences such as individuals possessing excessive amounts of control over each other should be avoided. For instance, Lyon (2001, p. 2) speaks of the dual aspects of surveillance in that "[t]he same process, surveillance – watching over – both enables and constrains, involves care and control." Michael et al. (2006a) reinforce such ideas in the context of GPS tracking

and monitoring. The authors claim that GPS tracking has been employed for control purposes in various situations, such as policing/law enforcement, the monitoring of parolees and sex offenders, the tracking of suspected terrorists and the monitoring of employees (Michael et al. 2006a, pp. 2-3). However, the authors argue that additional contexts such as convenience and care must not be ignored, as GPS solutions may potentially simplify or enable daily tasks (convenience) or be used for healthcare or protection of vulnerable groups (care) (Michael et al. 2006a, pp. 3-4). Perusco and Michael (2005) further note that the tracking of such vulnerable groups indicates that monitoring activities are no longer limited to those convicted of a particular offence, but rather can be employed for protection and safety purposes. Table 1 provides a summary of GPS tracking and monitoring applications in the control, convenience and care contexts, adapted from Michael et al. (2006a, pp. 2-4), identifying the potentially constructive uses of GPS tracking and monitoring.

Table 1: GPS monitoring applications in the control, convenience and care contexts, adapted from Michael et al. (2006a, pp. 2-4)

Context	Applications
Control	Law enforcement Parolees and sex offenders tracking Suspected terrorists tracking Employee monitoring
Convenience	Vehicle tracking Child/family member/friend tracking Sport-related applications
Care	Monitoring of dementia sufferers Child tracking

It is crucial that in evaluating LBS control literature and establishing the need for LBS regulation, both the control and care perspectives are incorporated. The act of monitoring should not immediately conjure up sinister thoughts. The focus should preferably be directed to the important question of purpose or motives. Lyon (2007, p. 3) feels that purpose may exist anywhere on the broad spectrum between care and control. Therefore, as expressed by Elliot and Phillips (2004, p. 474), a crucial factor in evaluating the merit of surveillance activities and systems is determining "how they are used." These sentiments are also applicable to dataveillance. It is helpful at this point to discuss alternative and related practices that may incorporate location information throughout the monitoring process.

Sousveillance

The term sousveillance, coined by Steve Mann, comes from the French terms *sous* which means *from below*, and veiller which means *to watch* (Mann et al. 2003, p. 332). It is primarily a form of "inverse surveillance" (Mann et al. 2003, p. 331), whereby an individual is in essence "surveilling the surveillers" (p. 332). Sousveillance is reliant on the use of wearable computing devices to capture *audiovisual* and *sensory* data (Mann 2005, p. 625). A major concern with respect to sousveillance, according to Mann (2005, p. 637), is the dissemination of the recorded data which for the purposes of this investigation, may include images of locations and corresponding geographic coordinates.

Sousveillance, 'reflectionism' and control

Relevant to the theme of control, it has been argued that sousveillance can be utilised as a form of resistance to unwarranted surveillance and control by institutions. According to Mann et al. (2003, p. 333), sousveillance is a type of reflectionism in which individuals can actively respond to bureaucratic monitoring and to an extent

"neutralize surveillance". Sousveillance can thus be employed in response to social control in that surveillance activities are reversed:

> *"The surveilled become sousveillers who engage social controllers (customs officials, shopkeepers, customer service personnel, security guards, etc.) by using devices that mirror those used by these social controllers"* (Mann et al. 2003, p. 337).

Sousveillance differs from surveillance in that traditional surveillance activities are "centralised" and "localized." It is dispersed in nature and "delocalized" in its global coverage (Ganascia 2010, p. 496). As such, sousveillance requires new metaphors for understanding its fundamental aspects. A useful metaphor proposed by Ganascia (2010, p. 496) for describing sousveillance is the canopticon, which can be contrasted to the panopticon metaphor. At the heart of the canopticon are the following principles:

> *"total transparency of society, fundamental equality, which gives everybody the ability to watch – and consequently to control – everybody else, [and] total communication, which enables everyone to exchange with everyone else"* (Ganascia 2010, p. 497).

This exchange may include the dissemination of location details, thus signalling the need to incorporate sousveillance into LBS regulatory discussions. A noteworthy element of sousveillance is that it shifts the ability to control from the state/institution (surveillance) to the individual. While this can initially be perceived as an empowering feature, excessive amounts of control, if unchecked, may prove detrimental. That is, control may be granted to individuals to disseminate their location (and other) information, or the information of others, without the necessary precautions in place and in an unguarded fashion. The implications of this exercise are sinister in their extreme forms. When considered within the context of IoT, sousveillance ideals are likely compromised. Yes, I can fight back against state control and big brother with sousveillance but in doing so I unleash potentially a thousand or more little brothers, each with their capacity to (mis)use the information being gathered.

Towards überveillance

The concepts of surveillance, dataveillance and sousveillance have been examined with respect to their association with location services in an IoT world. It is therefore valuable, at this point, to introduce the related notion of überveillance. Überveillance, a term coined by M.G. Michael in 2006, can be described as "an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body" (Michael et al. 2006b; Macquarie Dictionary 2009, p. 1094). Überveillance combines the dimensions of identification, location and time, potentially allowing for forecasting and uninterrupted real-time monitoring (Michael and Michael 2007, pp. 9-10), and in its extreme forms can be regarded as "Big Brother on the inside looking out" (p. 10).

Überveillance is considered by several authors to be the contemporary notion that will supplant surveillance. For instance, Clarke (2007a, p. 27) suggests that the concept of surveillance is somewhat outdated and that contemporary discussions be focussed on the notion of überveillance. It has further been suggested that überveillance is built on the existing notion of dataveillance. That is, "[ü]berveillance takes that which was static or discrete in the dataveillance world, and makes it constant and embedded" (Michael and Michael 2007, p. 10). The move towards überveillance thus marks the evolution from physical, visual forms of monitoring (surveillance), through to the increasingly sophisticated and ubiquitous embedded chips (überveillance) (Michael & Michael 2010; Gagnon et al. 2013). Albrecht and McIntyre (2005) describe these embedded chips as "spychips" and were focused predominantly on RFID tracking of people through retail goods and services. They spend considerable space describing the Internet of Things concept. Perakslis and Wolk (2006) studied the social acceptance of RFID implants as a security method and Perakslis later went on to incorporate überveillance into her research into behavioural motivators and personality factors toward adoption of humancentric IoT applications.

Given that überveillance is an emerging term (Michael and Michael 2007, p. 9), diverse interpretations have been proposed. For example, Clarke (2007a) offers varying definitions of the term, suggesting that überveillance can be understood as any of the following: *omni-surveillance*, an apocalyptic notion that "applies across all space and all time (omnipresent), and supports some organisation that is all-seeing and even all-knowing (omniscient)", which can be achieved through the use of embedded chips for instance (p. 33); *exaggerated surveillance*, referring to "the extent to which surveillance is undertaken... its justification is exaggerated" (p. 34) ; and/or *meta-, supra-, or master-surveillance*, which "could involve the consolidation of multiple surveillance threads in order to develop what would be envisaged by its proponents to be superior information" (p. 38). Shay et al. (2012) acknowledge:

> *"The pervasive nature of sensors coupled with recent advances in data mining, networking, and storage technologies creates tools and data that, while serving the public good, also create a ubiquitous surveillance infrastructure ripe for misuse. Roger Clarke's concept of dataveillance and M.G. Michael and Katina Michael's more recent uberveillance serve as important milestones in awareness of the growing threat of our instrumented world."*

All of these definitions indicate direct ways in which IoT applications can also be rolled-out whether it is for use of vehicle management in heavy traffic conditions, the tracking of suspects in a criminal investigation or even employees in a workplace. Disturbing is the manner in which a whole host of applications, particularly in tollways and public transportation, are being used for legal purposes without the knowledge of the driver and commuter. "Tapping" token cards is not only encouraged but mandatory at most metropolitan train stations of developed countries. Little do commuters know that the data gathered by these systems can be requested by a host of government agencies without a warrant.

Implications of überveillance on control

Irrespective of interpretation, the subject of current scholarly debate relates to the implications of überveillance on individuals in particular, and society in general. In an article discussing the evolution of automatic identification (auto-ID) techniques, Michael and Michael (2005) present an account of the issues associated with implantable technologies in humancentric applications. The authors note the evident trend of deploying a technology into the marketplace, prior to assessing the potential consequences (Michael and Michael 2005, pp. 22-33). This reactive approach causes apprehension in view of chip implants in particular, given the inexorable nature of embedded chips, and the fact that once the chip is accepted by the body, it is impossible to remove without an invasive surgical procedure, as summarised in the following excerpt:

> *"[U]nless the implant is removed within a short time, the body will adopt the foreign object and tie it to tissue. At this moment, there will be no exit strategy, no contingency plan, it will be a life enslaved to upgrades, virus protection mechanisms, and inescapable intrusion"* (Michael and Michael 2007, p. 18).

Other concerns relevant to this investigation have also been raised. It is indicated that "über-intrusive technologies" are likely to leave substantial impressions on individuals, families and other social relations, with the added potential of affecting psychological well-being (Michael and Michael 2007, p. 17). Apart from implications for individuals, concerns also emerge at the broader social level that require remedies. For instance, if a state of überveillance is to be avoided, caution must be exercised in deploying technologies without due reflection of the corresponding implications. Namely, this will involve the introduction of appropriate regulatory measures, which will encompass proactive consideration of the social implications of emerging technologies and individuals assuming responsibility for promoting regulatory measures (Michael and Michael 2007, p. 20). It will also require a measured attempt to achieve some form of "balance" (Clarke 2007a, p. 43). The implications of überveillance are of particular relevance to LBS regulatory discussions, given that "overarching location tracking and monitoring is leading toward a state of überveillance" (Michael and Michael 2011, p. 2). As such, research into LBS regulation in Australia must be sensitive to both the significance of LBS to überveillance and the anticipated trajectory of the latter.

Unfortunately the same cannot be said for IoT-specific regulation. IoT is a fluid concept, and in many ways IoT is nebulous. It is made up of a host of technologies that are being integrated and are converging together over time. It is layers upon layers of infrastructure which have emerged since the inception of the first telephone lines to the cloud and wireless Internet today. IoT requires new protocols and new applications but it is difficult to point to a specific technology or application or system that can be subject to some form of external oversight. Herein lie the problems of potential unauthorised disclosure of data, or even misuse of data when government agencies require private enterprise to act upon their requests, or private enterprises work together in sophisticated ways to exploit the consumer.

Comparing the different forms of 'veillance'

Various terms ending in 'veillance' have been introduced throughout this paper, all of which imply and encompass the process of monitoring. Prior to delving into the dangers of this activity and the significance of LBS monitoring on control, it is helpful to compare the main features of each term. A comparison of surveillance, dataveillance, sousveillance, and überveillance is provided in Table 2.

It should be noted that with the increased use of techniques such as surveillance, dataveillance, sousveillance and überveillance, the threat of becoming a *surveillance society* looms. According to Ganascia (2010p. 491), a surveillance society is one in which the data gathered from the aforementioned techniques is utilised to exert power and control over others. This results in dangers such as the potential for identification and profiling of individuals (Clarke 1997), the latter of which can be associated with social sorting (Gandy 1993).

Table 2: Comparison of the different forms of 'veillance'

Type of 'veillance'	Main systems/ technologies utilised	Primary focus
Surveillance	Visual monitoring systems	First hand observation/ images
Dataveillance	Automated, and therefore efficient, personal data collection systems	Data and aggregated data/information
Sousveillance	Wearable computing devices and technologies	Capture of audiovisual and sensory data, which may include location information
Überveillance	Embedded radio-frequency identification (RFID) chips	Identity and real-time location information

Identification

Identity and identification are ambiguous terms with philosophical and psychological connotations (Kodl and Lokay 2001, p. 129). Identity can be perceived as "a particular presentation of an entity, such as a role that the entity plays in particular circumstances" (Clarke and Wigan 2011). With respect to information systems, *human identification* specifically (as opposed to object identification) is therefore "the association of data with a particular human being" (Kodl and Lokay 2001, pp. 129-130). Kodl and Lokay (2001, pp. 131-135) claim that numerous methods exist to identify individuals prior to performing a data linkage, namely, using appearance, social interactions/behaviours, names, codes and knowledge, amongst other techniques. With respect to LBS, these *identifiers* significantly contribute to the dangers pertaining to surveillance, dataveillance, souseveillance and überveillance. That is, LBS can be deployed to simplify and facilitate the process of tracking and be used

for the collection of profile data that can potentially be linked to an entity using a given identification scheme. In a sense, LBS in their own right become an additional form of identification feeding the IoT scheme (Michael and Michael, 2013).

Thus, in order to address the regulatory concerns pertaining to LBS, it is crucial to appreciate the challenges regarding the identification of individuals. Of particularly importance is recognition that once an individual has been identified, they can be subjected to varying degrees of control. As such, in any scheme that enables identification, Kodl and Lokay (2001, p. 136) note the need to balance human rights with other competing interests, particularly given that identification systems may be exploited by powerful entities for control purposes, such as by governments to exercise social control. For an historical account of identification techniques, from manual methods through to automatic identification systems including those built on LBS see Michael and Michael (2009, pp. 43-60). It has also been suggested that civil libertarians and concerned individuals assert that automatic identification (auto-ID) technology "impinges on human rights, the right to privacy, and that eventually it will lead to totalitarian control of the populace that have been put forward since at least the 1970s" (Michael and Michael 2009, p. 364). These views are also pertinent to the notion of *social sorting*.

Social sorting

In relation to the theme of control, information derived from surveillance, dataveillance, sousveillance and überveillance techniques can also serve the purpose of social sorting, labelled by Oscar Gandy (1993, p. 1) as the "panoptic sort." Relevant to this discussion, the information may relate to an individual's location. In Gandy's influential work *The Panoptic Sort: A Political Economy of Personal Information*, the author relies on the work of Michel Foucault and other critical theorists (refer to pp. 3-13) in examining the panoptic sort as an "antidemocratic system of control" (Gandy 1993, p. 227). According to Gandy, in this system, individuals are exposed to prejudiced forms of categorisation based on both economic and political factors (pp. 1-2). Lyon (1998, p. 94) describes the database management practices associated with social sorting, classing them a form of *consumer surveillance*, in which customers are grouped by "social type and location." Such clustering forms the basis for the exclusion and marginalisation of individuals (King 2001, pp. 47-49). As a result, social sorting is presently used for profiling of individuals and in the market research realm (Bennett and Regan 2004, p. 452).

Profiling

Profiling "is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics" (Clarke 1993). The process is centred on the creation of a profile or model related to a specific individual, based on data aggregation processes (Casal 2004, p. 108). Assorted terms have been employed in labelling this profile. For instance, the model created of an individual using the data collected through dataveillance techniques has been referred to by Clarke (1997) as "the digital persona", and is related to the "digital dossiers" idea introduced by Solove (2004, pp. 1-7). According to Clarke (1994), the use of networked systems, namely the internet, involves communicating and exposing data and certain aspects of, at times, recognisable behaviour, both of which are utilised in the creation of a personality.

Digital personas and dossiers

The resulting personality is referred to as the digital persona. Similarly, *digital dossiers* refer to the compilation of comprehensive electronic data related to an individual, utilised in the creation of the "digital person" (Solove 2004, p. 1), also referred to as "digital biographies" (Solove 2002, p. 1086). Digital biographies are further discussed by Solove (2002). In examining the need for LBS regulation throughout the globe, a given regulatory response or framework must appreciate the ease with which (past, present and future) location information can be compiled and integrated into an individual's digital persona or dossier. Once such information is reproduced and disseminated the control implications are magnified.

With respect to the theme of control, an individual can exercise a limited amount of influence over their digital persona, as some aspects of creating an electronic personality may not be within their direct control. The scope of this article does not allow for reflection on the digital persona in great detail; however, Clarke (1994) offers a thorough investigation of the term, and associated notions such as the passive and active digital persona, in addition to the significance of the digital person to dataveillance techniques such as computer matching and profiling. However, significant to this research is the distinction between the physical and the digital persona and the resultant implications in relation to control, as summarised in the following extract:

> *"The physical persona is progressively being replaced by the digital persona as the basis for social control by governments, and for consumer marketing by corporations. Even from the strictly social control and business efficiency perspectives, substantial flaws exist in this approach. In addition, major risks to individuals and society arise"* (Clarke 1994).

The same sentiments apply with respect to digital dossiers. In particular, Solove (2004, p. 2) notes that individuals are unaware of the ways in which their electronic data is exploited by government and commercial entities, and "lack the power to do much about it." It is evident that profile data is advantageous for both social control and commercial purposes (Clarke 2001d, p. 12), the latter of which is associated with market research and sorting activities, which have evolved from ideas of "containment" of mobile consumer demand to the "control" model (Arvidsson 2004, pp. 456, 458-467). The control model in particular has been strengthened, but not solely driven, by emerging technologies including LBS, as explained:

> *"The control paradigm thus permits a tighter and more efficient surveillance that makes use of consumer mobility rather than discarding it as complexity. This ability to follow the consumer around has been greatly strengthened by new technologies: software for data mining, barcode scans, internet tracking devices, and lately location based information from mobile phones" (*Arvidsson 2004, p. 467).

Social sorting, particularly for profiling and market research purposes, thus introduces numerous concerns relating to the theme of control, one of which is the ensuing consequences relating to personal privacy. This specifically includes the privacy of location information. In sum, examining the current regulatory framework for LBS in Australia, and determining the need for LBS regulation, necessitates an appreciation of the threats associated with social sorting using information derived from LBS solutions. Additionally, the benefits and risks associated with surveillance, dataveillance, sousveillance and überveillance for control must be measured and carefully contemplated in the proposed regulatory response.

Trust

Trust is a significant theme relating to LBS, given the importance of the notion to: (a) "human existence" (Perusco et al. 2006, p. 93; Perusco and Michael 2007, p. 10), (b) relationships (Lewis and Weigert 1985, pp. 968-969), (c) intimacy and rapport within a domestic relationship (Boesen et al. 2010, p. 65), and (d) LBS success and adoption (Jorns and Quirchmayr 2010, p. 152). Trust can be defined, in general terms, as the "firm belief in the reliability, truth, or ability of someone or something" (Oxford Dictionary 2012b). A definition of trust that has been widely cited in relevant literature is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995, p. 712). Related to electronic relationships or transactions, the concept has been defined as the "confident reliance by one party on the behaviour of other parties" (Clarke 2001c, p. 291), and it has been suggested that in the electronic-commerce domain, in particular, trust is intimately associated with the disclosure of information (Metzger 2004).

In reviewing literature concerning trust, Fusco et al. (2011, p. 2) claim that trust is typically described as a dynamic concept falling into the categories of cognitive (evidence based), emotional (faith-based), and/or behavioural (conduct-based) trust. For further reading, the major sources on trust can be found in: Lewis and Weigert's (1985) sociological treatment of trust, the influential work of Mayer et al. (1995) and the authors' updated work Schoorman et al. (2007) centred on organisational trust, Weckert's (2000) comprehensive review

of trust in the context of workplace monitoring using electronic devices, research on trust in electronic-commerce (refer to McKnight and Chervany 2001; Pavlou 2003; Kim et al. 2009) and mobile-commerce (see Siau and Shen 2003; Yeh and Li 2009), the work of Valachich (2003) that introduces and evaluates trust in terms of ubiquitous computing environments, Dwyer et al.'s (2007) article on trust and privacy issues in social networks, Yan and Holtmanns' (2008) examination of issues associated with digital trust management, the work of Chen et al. (2008) covering the benefits and concerns of LBS usage including privacy and trust implications, and the research by Junglas and Spitzmüller (2005) that examines privacy and trust issues concerning LBS by presenting a research model that incorporates these aspects amongst others.

For the purpose of this paper, the varying definitions and categorisations are acknowledged. However, trust will be assessed in terms of the relationships dominating existing LBS/IoT scholarship which comprise the government-citizen relationship centred on trust in the state, the business-consumer relationship associated with trust in corporations/LBS providers, and the consumer-consumer relationship concerned with trust in individuals/others.

Trust in the state

Trust in the state broadly covers LBS solutions implemented by government, thus representing the government-citizen relationship. Dominating current debates and literature are LBS government initiatives in the form of emergency management schemes, in conjunction with national security applications utilising LBS, which depending on the nature of their implementation may impact on citizens' trust in the state. These concerns are typically expressed as a trade-off between security and safety. At present there are very few examples of fully-fledged IoT systems to point to, although increasingly quasi-IoT systems are being deployed using wireless sensor networks of varying kinds, e.g. for bushfire management and for fisheries. These systems do not include a direct human stakeholder but are still relevant as they may trigger flow-on effects that do impact citizenry.

Balancing trust and privacy in emergency services

In the context of emergency management, Aloudat and Michael (2011, p. 58) maintain that the dominant theme between government and consumers in relation to emergency warning messages and systems is trust. This includes trust in the LBS services being delivered and in the government itself (Aloudat and Michael 2011, p. 71). While privacy is typically believed to be the leading issue confronting LBS, in emergency and life-threatening situations it is overwhelmed by trust-related challenges, given that users are generally willing to relinquish their privacy in the interest of survival (Aloudat and Michael 2010, p. 2). Furthermore, the success of these services is reliant on trust in the technology, the service, and the accuracy/reliability/timeliness of the emergency alert. On the whole, this success can be measured in terms of citizens' confidence in their government's ability to sensibly select and implement a fitting emergency service utilising enhanced LBS features. In a paper that examines the deployment of location services in Dutch public administration, van Ooijen and Nouwt (2009, p. 81) assess the impact of government-based LBS initiatives on the government-citizen relationship, recommending that governments employ care in gathering and utilising location-based data about the public, to ensure that citizens' trust in the state is not compromised.

Trust-related implications of surveillance in the interest of national security

Trust is also prevalent in discussions relating to national security. National security has been regarded a priority area for many countries for over a decade, and as such has prompted the implementation of surveillance schemes by government. Wigan and Clarke (2006, p. 392) discuss the dimension of trust as a significant theme contributing to the social acceptance of a particular government surveillance initiative, which may incorporate location and tracking of individuals and objects. The implementation of surveillance systems by the state, including those incorporating LBS, can diminish the public's confidence in the state given the potential for such mechanisms to be perceived as a form of authoritarian control. Nevertheless, a situation where national security

and safety are considered to be in jeopardy may entail (partial) acceptance of various surveillance initiatives that would otherwise be perceived objectionable. In such circumstances, trust in government plays a crucial role in determining individuals' willingness to compromise various civil liberties. This is explained by Davis and Silver (2004, p. 35) below:

> *"The more people trust the federal government or law enforcement agencies, the more willing they are to allow the government leeway in fighting the domestic war on terrorism by conceding some civil liberties."*

However, in due course it is expected that such increased security measures (even if initially supported by citizens) will yield a growing gap between government and citizens, "potentially dampening citizen participation in government and with it reducing citizens' trust in public institutions and officials" (Gould 2002, p. 77). This is so as the degree of threat and trust in government is diminishing, thus resulting in the public's reluctance to surrender their rights for the sake of security (Sanquist et al. 2008, p. 1126). In order to build and maintain trust, governments are required to be actively engaged in developing strategies to build confidence in both their abilities and of the technology under consideration, and are challenged to recognise "the massive harm that surveillance measures are doing to public confidence in its institutions" (Wigan and Clarke 2006, p. 401). It has been suggested that a privacy impact assessment (PIA) aids in establishing trust between government and citizens (Clarke 2009, p. 129). Carefully considered legislation is an alternative technique to enhance levels of trust. With respect to LBS, governments are responsible for proposing and enacting regulation that is in the best interest of citizens, incorporating citizen concerns into this process and encouraging suitable design of LBS applications, as explained in the following quotation:

> *"...new laws and regulations must be drafted always on the basis of citizens' trust in government authorities. This means that citizens trust the government to consider the issues at stake according to the needs and wishes of its citizens. Location aware services can influence citizens' trust in the democratic society. Poorly designed infrastructures and services for storing, processing and distributing location-based data can give rise to a strong feeling of being threatened. Whereas a good design expands the feeling of freedom and safety, both in the private and in the public sphere/domain"* (Beinat et al. 2007, p. 46).

One of the biggest difficulties that will face stakeholders is identifying when current LBS systems become a part of bigger IoT initiatives. Major changes in systems will require a re-evaluation of impact assessments of different types.

Need for justification and cultural sensitivity

Techniques of this nature will fail to be espoused, however, if surveillance schemes lack adequate substantiation at the outset, as trust is threatened by "absence of justification for surveillance, and of controls over abuses" (Wigan and Clarke 2006, p. 389). From a government perspective, this situation may prove detrimental, as Wigan and Clarke (2006, p. 401) claim that transparency and trust are prerequisites for ensuring public confidence in the state, noting that "[t]he integrity of surveillance schemes, in transport and elsewhere, is highly fragile." Aside from adequate justification of surveillance schemes, cultural differences associated with the given context need to be acknowledged as factors influencing the level of trust citizens hold in government. As explained by Dinev et al. (2005, p. 3) in their cross-cultural study of American and Italian Internet users' privacy and surveillance concerns, "[a]ttitudes toward government and government initiatives are related to the culture's propensity to trust." In comparing the two contexts, Dinev et al. claim that Americans readily accept government surveillance to provide increased levels of security, whereas Italians' low levels of trust in government results in opposing viewpoints (pp. 9-10).

Trust in corporations/LBS/IoT providers

Trust in corporations/LBS/IoT providers emerges from the level of confidence a user places in an organisation and their respective location-based solution(s), which may be correlated to the business-consumer relationship. In the context of consumer privacy, Culnan and Bies (2003, p. 327) assert that perceived trust in an organisation is closely linked to the extent to which an organisation's practices are aligned with its policies. A breach in this trust affects the likelihood of personal information disclosure in the future (Culnan and Bies 2003, p. 328), given the value of trust in sustaining lasting customer relationships (p. 337). Reducing this "trust gap" (Culnan and Bies 2003, pp. 336-337) is a defining element for organisations in achieving economic and industry success, as it may impact on a consumer's decision to contemplate location data usage (Chen et al. 2008, p. 34). Reducing this gap requires that control over location details remain with the user, as opposed to the LBS provider or network operator (Giaglis et al. 2003, p. 82). Trust can thus emerge from a user's perception that they are in command (Junglas and Spitzmüller 2005, p. 3).

Küpper and Treu (2010, pp. 216-217) concur with these assertions, explaining that the lack of uptake of first-generation LBS applications was chiefly a consequence of the dominant role of the network operator over location information. This situation has been somewhat rectified since the introduction of GPS-enabled devices capable of determining location information without input from the network operator and higher emphasis on a user-focussed model (Bellavista et al. 2008, p. 85; Küpper and Treu 2010, p. 217). Trust, however, is not exclusively concerned with a network operator's ability to determine location information, but also with the possible misuse of location data. As such, it has also been framed as a potential resolution to location data misappropriation, explained further by Jorns and Quirchmayr (2010, p. 152) in the following excerpt:

> *"The only way to completely avoid misuse is to entirely block location information, that is, to reject such services at all. Since this is not an adequate option... trust is the key to the realization of mobile applications that exchange sensitive information."*

There is much to learn from the covert and overt location tracking of large corporation on their subscribers. Increasingly, the dubious practices of retaining location information by information and communication technology giants Google, Apple and Microsoft are being reported and only small commensurate penalties being applied in countries in the European Union and Asia. Disturbing in this trend is that even smaller suppliers of location-based applications are beginning to unleash unethical (but seemingly not illegal) solutions at shopping malls and other campus-based locales (Michael & Clarke 2013).

Importance of identity and privacy protection to trust

In delivering trusted LBS solutions, Jorns and Quirchmayr (2010, pp. 151-155) further claim that identity and privacy protection are central considerations that must be built into a given solution, proposing an LBS architecture that integrates such safeguards. That is, identity protection may involve the use of false dummies, dummy users and landmark objects, while privacy protection generally relies on decreasing the resolution of location data, employing supportive regulatory techniques and ensuring anonymity and pseudonymity (Jorns and Quirchmayr 2010, p. 152). Similarly, and with respect to online privacy, Clarke (2001c, p. 297) suggests that an adequate framework must be introduced that "features strong and comprehensive privacy laws, and systematic enforcement of those laws." These comments, also applicable to LBS in a specific sense, were made in the context of economic rather than social relationships, referring primarily to government and corporations, but are also relevant to trust amongst social relations.

It is important to recognise that issues of trust are closely related to privacy concerns from the perspective of users. In an article titled, "Trust and Transparency in Location-Based Services: Making Users Lose their Fear of Big Brother", Böhm et al. (2004, pp. 1-3) claim that operators and service providers are charged with the difficult task of earning consumer trust and that this may be achieved by addressing user privacy concerns and adhering to relevant legislation. Additional studies also point to the relationship between trust and privacy, claiming that trust can aid in reducing the perceived privacy risk for users. For example, Xu et al. (2005) suggest

that enhancing trust can reduce the perceived privacy risk. This influences a user's decision to disclose information, and that "service provider's interventions including joining third party privacy seal programs and introducing device-based privacy enhancing features could increase consumers' trust beliefs and mitigate their privacy risk perceptions" (Xu et al. 2005, p. 905). Chellappa and Sin (2005, pp. 188-189), in examining the link between trust and privacy, express the importance of trust building, which include consumer's familiarity and previous experience with the organisation.

Maintaining consumer trust

The primary consideration in relation to trust in the business-consumer relationship is that all efforts be targeted at establishing and building trust in corporations and LBS/IoT providers. Once trust has been compromised, the situation cannot be repaired which is a point applicable to trust in any context. This point is explained by Kaasinen (2003, p. 77) in an interview-based study regarding user requirements in location-aware mobile applications:

> *"The faith that the users have in the technology, the service providers and the policy-makers should be regarded highly. Any abuse of personal data can betray that trust and it will be hard to win it back again."*

Trust in individuals/others

Trust in the consumer-to-consumer setting is determined by the level of confidence existing between an individual and their social relations, which may include *friends, parents, other family members, employers* and *strangers*, categories that are adapted from Levin et al. (2008, pp. 81-82). Yan and Holtmanns (2008, p. 2) express the importance of trust for social interactions, claiming that "[s]ocial trust is the product of past experiences and perceived trustworthiness." It has been suggested that LBS monitoring can erode trust between the individual engaged in monitoring and the subject being monitored, as the very act implies that trust is lacking in a given relationship (Perusco et al. 2006, p. 93). These concerns are echoed in Michael et al. (2008). Previous studies relevant to LBS and trust generally focus on: the workplace situation, that is, trust between an employer and their employee; trust amongst 'friends' subscribed to a location-based social networking (LBSN) service which may include any of the predefined categories above; in addition to studies relating to the tracking of family members, such as children for instance, for safety and protection purposes and the relative trust implications.

Consequences of workplace monitoring

With respect to trust in an employer's use of location-based applications and location data, a prevailing subject in existing literature is the impact of employee monitoring systems on staff. For example, in studying the link between electronic workplace monitoring and trust, Weckert (2000, p. 248) reported that trust is a significant issue resulting from excessive monitoring, in that monitoring may contribute to deterioration in professional work relationships between an employer and their employee and consequently reduce or eliminate trust. Weckert's work reveals that employers often substantiate electronic monitoring based on the argument that the "benefits outweigh any loss of trust", and may include gains for the involved parties; notably, for the employer in the form of economic benefits, for the employee to encourage improvements to performance and productivity, and for the customer who may experience enhanced customer service (p. 249). Chen and Ross (2005, p. 250), on the other hand, argue that an employer's decision to monitor their subordinates may be related to a low degree of existing trust, which could be a result of unsuitable past behaviour on the part of the employee. As such, employers may perceive monitoring as necessary in order to manage employees. Alternatively, from the perspective of employees, trust-related issues materialise as a result of monitoring, which may leave an impression on job attitudes, including satisfaction and dedication, as covered in a paper by Alder et al. (2006) in the context of internet monitoring.

When applied to location monitoring of employees using LBS, the trust-related concerns expressed above are indeed warranted. Particularly, Kaupins and Minch (2005, p. 2) argue that the appropriateness of location monitoring in the workplace can be measured from either a legal or ethical perspective, which inevitably results in policy implications for the employer. The authors emphasise that location monitoring of employees can often be justified in terms of the security, productivity, reputational and protective capabilities of LBS (Kaupins and Minch 2005, p. 5). However, Kaupins and Minch (2005, pp. 5-6) continue to describe the ethical factors "limiting" location monitoring in the workplace, which entail the need for maintaining employee privacy and the restrictions associated with inaccurate information, amongst others. These factors will undoubtedly affect the degree of trust between an employer and employee.

However, the underlying concern relevant to this discussion of location monitoring in the workplace is not only the suitability of employee monitoring using LBS. While this is a valid issue, the challenge remains centred on the deeper trust-related consequences. Regardless of the technology or applications used to monitor employees, it can be concluded that a work atmosphere lacking trust results in sweeping consequences that extend beyond the workplace, expressed in the following excerpt:

> *"A low trust workplace environment will create the need for ever increasing amounts of monitoring which in turn will erode trust further. There is also the worry that this lack of trust may become more widespread. If there is no climate of trust at work, where most of us spend a great deal of our life, why should there be in other contexts? Some monitoring in some situations is justified, but it must be restricted by the need for trust"* (Weckert 2000, p. 250).

Location-monitoring amongst friends

Therefore, these concerns are certainly applicable to the use of LBS applications amongst other social relations. Recent literature merging the concepts of LBS, online social networking and trust are particularly focused on the use of LBSN applications amongst various categories of *friends*. For example, Fusco et al.'s (2010) qualitative study examines the impact of LBSN on trust amongst friends, employing a focus group methodology in achieving this aim. The authors reveal that trust may suffer as a consequence of LBSN usage in several ways: as disclosure of location information and potential monitoring activities can result in application misuse in order to conceal things; excessive questioning and the deterioration in trust amongst social relations; and trust being placed in the application rather than the friend (Fusco et al. 2010, p. 7). Further information relating to Fusco et al.'s study, particularly the manner in which LBSN applications adversely impact on trust can be found in a follow-up article (Fusco et al. 2011).

Location tracking for protection

It has often been suggested that monitoring in familial relations can offer a justified means of protection, particularly in relation to vulnerable individuals such as Alzheimer's or dementia sufferers and in children. With specific reference to the latter, trust emerges as a central theme relating to child tracking. In an article by Boesen et al. (2010) location tracking in families is evaluated, including the manner in which LBS applications are incorporated within the familial context. The qualitative study conducted by the authors revealed that the initial decision to use LBS by participants with children was a lack of existing trust within the given relationship, with participants reporting an improvement in their children's behaviour after a period of tracking (Boesen et al. 2010, p. 70). Boesen et al., however, warn of the trust-related consequences, claiming that "daily socially-based trusting interactions are potentially replaced by technologically mediated interactions" (p. 73). Lack of trust in a child is considered to be detrimental to their growth. The act of nurturing a child is believed to be untrustworthy through the use of technology, specifically location monitoring applications, may result in long-term implications. The importance of trust to the growth of a child and the dangers associated with ubiquitous forms of supervision are explained in the following excerpt:

> *"Trust (or at least its gradual extension as the child grows) is seen as fundamental to emerging self-control and healthy development... Lack of private spaces (whether physical, personal or social) for*

> *children amidst omni-present parental oversight may also create an inhibiting dependence and fear"* (Marx and Steeves 2010, p. 218).

Furthermore, location tracking of children and other individuals in the name of protection may result in undesirable and contradictory consequences relevant to trust. Barreras and Mathur (2007, p. 182), in an article that describes the advantages and disadvantages of wireless location tracking, argue that technologies originally intended to protect family members (notably children, and other social relations such as friends and employees), can impact on trust and be regarded as "unnecessary surveillance." The outcome of such tracking and reduced levels of trust may also result in a "counterproductive" effect if the tracking capabilities are deactivated by individuals, rendering them incapable of seeking assistance in actual emergency situations (Barreras and Mathur 2007, p. 182).

LBS/IoT is a 'double-edged sword'

In summary, location monitoring and tracking by the state, corporations and individuals is often justified in terms of the benefits that can be delivered to the party responsible for monitoring/tracking and the subject being tracked. As such, Junglas and Spitzmüller (2005, p. 7) claim that location-based services can be considered a "double-edged sword" in that they can aid in the performance of tasks in one instance, but may also generate Big Brother concerns. Furthermore, Perusco and Michael (2007, p. 10) mention the linkage between trust and freedom. As a result, Perusco et al. (2006, p. 97) suggest a number of questions that must be considered in the context of LBS and trust: "Does the LBS context already involve a low level of trust?"; "If the LBS context involves a moderate to high level of trust, why are LBS being considered anyway?"; and "Will the use of LBS in this situation be trust-building or trust-destroying?" In answering these questions, the implications of LBS/IoT monitoring on trust must be appreciated, given they are significant, irreparable, and closely tied to what is considered the central challenge in the LBS domain, privacy.

This paper has provided comprehensive coverage of the themes of control and trust with respect to the social implications of LBS. The subsequent discussion will extend the examination to cover LBS in the context of the IoT, providing an ethical analysis and stressing the importance of a robust socio-ethical framework.

Discussion

The Internet of Things (IoT) and LBS: extending the discussion on control and trust

The Internet of Things (IoT) is an encompassing network of connected intelligent "things", and is "comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures" (Freescale Semiconductor Inc. and ARM Inc. 2014, p. 1). The phrase was originally coined by Kevin Ashton in 1999, and a definite definition is yet to be agreed upon (Ashton 2009, p. 1; Kranenburg and Bassi 2012, p. 1). Various forms of IoT are often used interchangeably, such as the Internet of Everything, the Internet of Things and People, the Web of Things and People etc. The IoT can, however, be described in terms of its core characteristics and/or the features it encompasses. At the crux of the IoT concept is the integration of the physical and virtual worlds, and the capability for "things" within these realms to be operated remotely through the employment of intelligent or smart objects with embedded processing functionality (Mattern and Floerkemeier 2010, p. 242; Ethics Subgroup IoT 2013, p. 3). These smart objects are capable of storing historical and varied forms of data, used as the basis for future interactions and the establishment of preferences. That is, once the data is processed, it can be utilized to "command and control" things within the IoT ecosystem, ideally resulting in enhancing the everyday lives of individual (Michael, K. et al., 2010).

According to Ashton (2009, p. 1), the IoT infrastructure should "empower computers" and exhibit less reliance on human involvement in the collection of information. It should also allow for "seamless" interactions and connections (Ethics Subgroup IoT 2013, p. 2). Potential use cases include personal/home applications,

health/patient monitoring systems, and remote tracking and monitoring which may include applications such as asset tracking amongst others (Ethics Subgroup IoT 2013, p. 3).

As can be anticipated with an ecosystem of this scale, the nature of interactions with the physical/virtual worlds and the varied "things" within, will undoubtedly be affected and dramatically alter the state of play. In the context of this paper, the focus is ultimately on the ethical concerns emerging from the use of LBS within the IoT infrastructure that is characterized by its ubiquitous/pervasive nature, in view of the discussion above regarding control and trust. It is valuable at this point to identify the important role of LBS in the IoT infrastructure.

While the IoT can potentially encompass a myriad of devices, the mobile phone will likely feature as a key element within the ecosystem, providing connectivity between devices (Freescale Semiconductor Inc. and ARM Inc. 2014, p. 2). In essence, smart phones can therefore be perceived as the "mediator" between users, the internet and additional "things", as is illustrated in Mattern and Floerkemeier (2010, p. 245, see figure 2). Significantly, most mobile devices are equipped with location and spatial capabilities, providing "localization", whereby intelligent devices "are aware of their physical location, or can be located" (Mattern and Floerkemeier 2010, p. 244). An example of an LBS application in the IoT would be indoor navigation capabilities in the absence of GPS; or in affect seamless navigation between the outdoor and indoor environments.

Control- and trust-related challenges in the IoT

It may be argued that the LBS control and trust implications discussed throughout this paper (in addition to ethical challenges such as privacy and security) will matriculate into the IoT environment. However, it has also been suggested that "the IoT will essentially create much richer environments in which location-based and location-aware technology can function" (Blouin 2014), and in doing so the ethical challenges will be amplified. It has further been noted that ethical issues, including trust and control amongst others, will "gain a new dimension in light of the increased complexity" in the IoT environment (Ethics Subgroup IoT 2013, p. 2).

In relation to control and the previously identified surveillance metaphors, for instance, it is predicted that there will be less reliance on Orwell's notion of Big Brother whereby surveillance is conducted by a single entity. Rather the concept of "some brother" will emerge. Some brother can be defined as "a heterogeneous 'mass' consisting of innumerable social actors, e.g. public sector authorities, citizens' movements and NGOs, economic players, big corporations, SMEs and citizens" (Ethics Subgroup IoT 2013, p. 16). As can be anticipated, the ethical consequences and dangers can potentially multiply in such a scenario.

Following on from this idea, is that of lack of transparency. The IoT will inevitably result in the merging of both the virtual and physical worlds, in addition to public and private spaces. It has been suggested that lack of transparency regarding information access will create a sense of discomfort and will accordingly result in diminishing levels of trust (Ethics Subgroup IoT 2013, p. 8). The trust-related issues (relevant to LBS) are likely to be consistent with those discussed throughout this paper, possibly varying in intensity/severity depending on a given scenario. For example, the consequences of faulty IoT technology have the potential to be greater than those in conventional Internet services given the integration of the physical and virtual worlds, thereby impact on users' trust in the IoT (Ethics Subgroup IoT 2013, p. 11). Therefore, trust considerations must primarily be examined in terms of: (a) trust in technology, and (b) trust in individuals/others.

Dealing with these (and other) challenges requires an ethical analysis in which appropriate conceptual and practical frameworks are considered. A preliminary examination is provided in the subsequent section, followed by dialogue regarding the need for objectivity in socio-ethical studies and the associated difficulties in achieving this.

Ethical analysis: proposing a socio-ethical conceptual framework

Research into the social and ethical implications of LBS, emerging technologies in general, and the IoT can be categorized in many ways and many frameworks can be applied. For instance, it may be regarded as a strand of "cyberethics", defined by Tavani (2007, p. 3) as "the study of moral, legal and social issues involving cybertechnology". Cybertechnology encompasses technological devices ranging from individual computers through to networked information and communication technologies. When considering ethical issues relating to cybertechnology and technology in general, Tavani (2007, pp. 23-24) notes that the latter should not necessarily be perceived as neutral. That is, technology may have "embedded values and biases" (Tavani 2007, p. 24), in that it may inherently provide capabilities to individuals to partake in unethical activities. This sentiment is echoed by Wakunuma and Stahl (2014, p. 393) in a paper examining the perceptions of IS professionals in relation to emerging ethical concerns.

Alternatively, research in this domain may be classed as a form of "computer ethics" or "information ethics", which can be defined and applied using numerous approaches. While this article does not attempt to provide an in-depth account of information ethics, a number of its crucial characteristics are identified. In the first instance, the value of information ethics is in its ability to provide a conceptual framework for understanding the array of ethical challenges stemming from the introduction of new ICTs (Mathiesen 2004, p. 1). According to Floridi (1999), the question at the heart of information ethics is "what is good for an information entity and the infosphere in general?" The author continues that "more analytically, we shall say that [information ethics] determines what is morally right or wrong, what ought to be done, what the duties, the 'oughts' and the 'ought nots' of a moral agent are…" However, Capurro (2006, p. 182) disagrees, claiming that information ethics is additionally about "what is good for our bodily being-in-the-world with others in particular?" This involves contemplation of other "spheres" such as the ecological, political, economic, and cultural and is not limited to a study of the infosphere as suggested by Floridi. In this sense, the significance of context, environment and intercultural factors also becomes apparent.

Following on from these notions, there is the need for a robust ethical framework that is multi-dimensional in nature and explicitly covers the socio-ethical challenges emerging from the deployment of a given technology. This would include, but not be limited to, the control and trust issues identified throughout this paper, other concerns such as privacy and security, and any challenges that emerge as the IoT takes shape. This article proposes a broader more robust socio-ethical conceptual framework, as an appropriate means of examining and addressing ethical challenges relevant to LBS; both LBS in general and as a vital mediating component within the IoT. This framework is illustrated in Figure 1. Central to the socio-ethical framework is the contemplation of individuals as part of a broader social network or society, whilst considering the interactions amongst various elements of the overall "system". The four themes underpinning socio-ethical studies include the investigation of what the human purpose is, what is moral, how justice is upheld and the principles that guide the usage of a given technique. Participants; their interactions with systems; people concerns and behavioural expectations; cultural and religious belief; structures, rules and norms; and fairness, personal benefits and personal harms are all areas of interest in a socio-ethical approach.

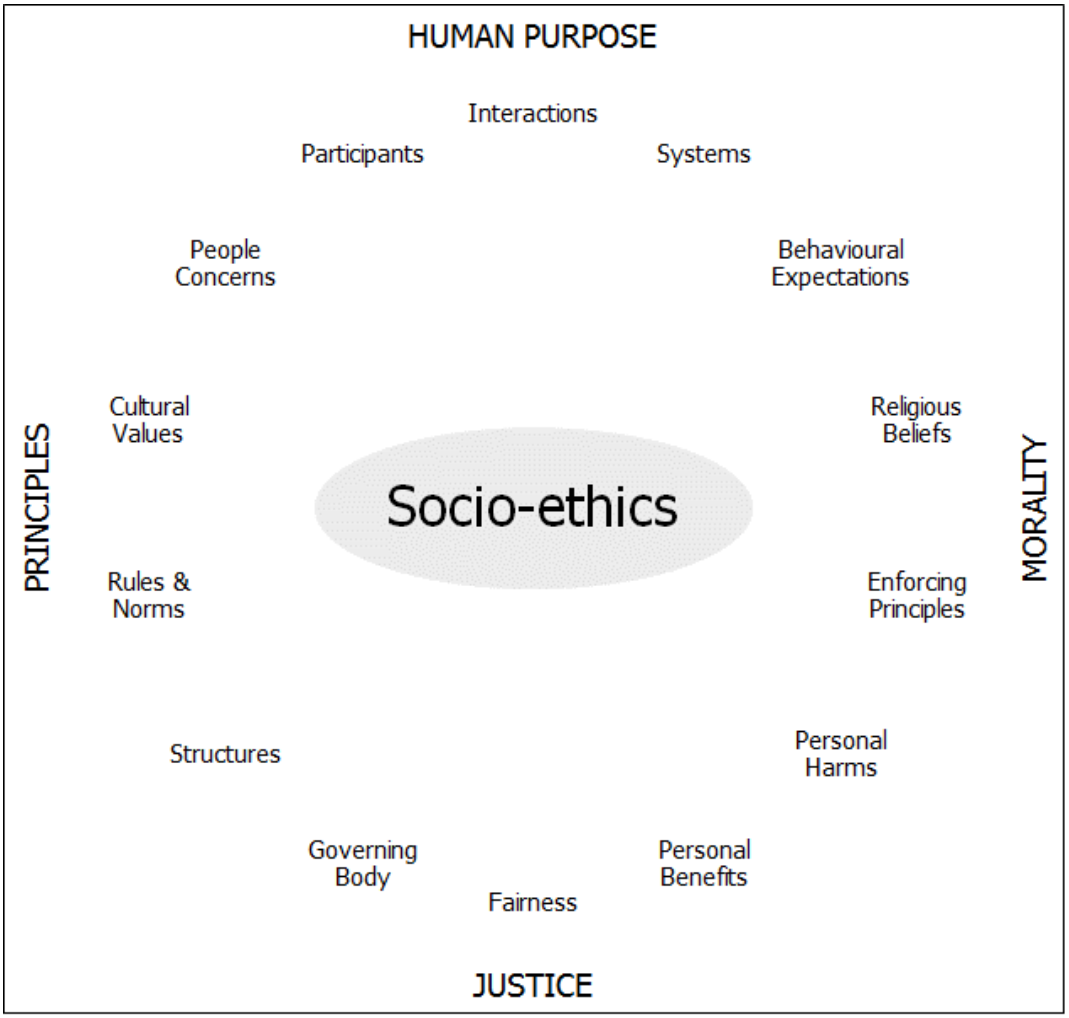

Figure 1: Proposed socio-ethical framework, in terms of the major components that require consideration

This article is intended to offer a preliminary account of the socio-ethical conceptual framework being proposed. Further research would examine and test its validity, whilst also providing a more detailed account of the various components within and how a socio-ethical assessment would be conducted based on the framework, and the range of techniques that could be applied.

The need for objectivity

Regardless of categorization and which conceptual framework is adopted, numerous authors stress that the focus of research and debates should not be skewed towards the unethical uses of a particular technology, but rather an objective stance should be embraced. Such objectivity must nonetheless ensure that social interests are adequately represented. That is, with respect to location and tracking technologies, Clarke (2001b, p. 220) claims that social interests have been somewhat overshadowed by the economic interests of LBS organisation. This is a situation that requires rectifying. While information technology professionals are not necessarily liable for how technology is deployed, they must nonetheless recognise its implications and be engaged in the process of introducing and promoting adequate safeguards (Clarke 1988, pp. 510-511). It has been argued that IS professionals are generally disinterested in the ethical challenges associated with emerging ICTs, and are rather concerned with the job or the technologies themselves (Wakunuma and Stahl 2014, p. 383).

This is explicitly the case for LBS given that the industry and technology have developed quicker than equivalent social implications scholarship and research, an unfavourable situation given the potential for LBS to have

profound impacts on individuals and society (Perusco et al. 2006, p. 91). In a keynote address centred on defining the emerging notion of überveillance, Clarke (2007a, p. 34) discusses the need to measure the costs and disbenefits arising from surveillance practices in general, where costs refer to financial measures, and disbenefits to all non-economic impacts. This involves weighing the negatives against the potential advantages, a response that is applicable to LBS, and pertinent to seeking objectivity.

Difficulties associated with objectivity

However, a major challenge with respect to an impartial approach for LBS is the interplay between the constructive and the potentially damaging consequences that the technology facilitates. For instance, and with specific reference to wireless technologies in a business setting, Elliot and Phillips (2004, p. 474) maintain that such systems facilitate monitoring and surveillance which can be applied in conflicting scenarios. Positive applications, according to Elliot and Phillips, include monitoring to improve effectiveness or provide employee protection in various instances, although this view has been frequently contested. Alternatively, negative uses involve excessive monitoring, which may compromise privacy or lead to situations in which an individual is subjected to surveillance or unauthorised forms of monitoring.

Additional studies demonstrate the complexities arising from the dual, and opposing, uses of a single LBS solution. It has been illustrated that any given application, for instance, parent, healthcare, employee and criminal tracking applications, can be simultaneously perceived as ethical and unethical (Michael et al. 2006a, p. 7). A closer look at the scenario involving parents tracking children, as explained by Michael et al. (2006a, p. 7), highlights that child tracking can enable the safety of a child on the one hand, while invading their privacy on the other. Therefore, the dual and opposing uses of a single LBS solution become problematic and situation-dependent, and indeed increasingly difficult to objectively examine. Dobson and Fischer (2003, p. 50) maintain that technology cannot be perceived as either good or evil in that it is not directly the cause of unethical behaviour, rather they serve to "empower those who choose to engage in good or bad behaviour."

This is similarly the case in relation to the IoT, as public approval of the IoT is largely centred on "the conventional dualisms of 'security versus freedom' and 'comfort versus data privacy'" (Mattern and Floerkemeier 2010, p. 256). Assessing the implications of the IoT infrastructure as a whole is increasingly difficult.

An alternative obstacle is associated with the extent to which LBS threaten the integrity of the individual. Explicitly, the risks associated with location and tracking technologies "arise from individual technologies and the trails that they generate, from compounds of multiple technologies, and from amalgamated and cross-referenced trails captured using multiple technologies and arising in multiple contexts" (Clarke 2001b, pp. 218). The consequent social implications or "dangers" are thus a product of individuals being convicted, correctly or otherwise, of having committed a particular action (Clarke 2001b, p. 219). A wrongly accused individual may perceive the disbenefits arising from LBS as outweighing the benefits.

However, in situations where integrity is not compromised, an LBS application can be perceived as advantageous. For instance, Michael et al. (2006, pp. 1-11) refer to the potentially beneficial uses of LBS, in their paper focusing on the Avian Flu Tracker prototype that is intended to manage and contain the spread of the infectious disease, by relying on spatial data to communicate with individuals in the defined location. The authors demonstrate that their proposed system which is intended to operate on a subscription or opt-in basis is beneficial for numerous stakeholders such as government, health organisations and citizens (Michael et al. 2006c, p. 6).

Thus, a common challenge confronting researchers with respect to the study of morals, ethics and technology is that the field of ethics is subjective. That is, what constitutes right and wrong behaviour varies depending on the beliefs of a particular individual, which are understood to be based on cultural and other factors specific to the individual in question. One such factor is an individual's experience with the technology, as can be seen in the previous example centred on the notion of an unjust accusation. Given these subjectivities and the potential for inconsistency from one individual to the next, Tavani (2007, p. 47) asserts that there is the need for ethical theories to direct the analysis of moral issues (relating to technology), given that numerous complications or disagreements exist in examining ethics.

Conclusion

This article has provided a comprehensive review of the control- and trust-related challenges relevant to location-based services, in order to identify and describe the major social and ethical considerations within each of the themes. The relevance of the IoT in such discussions has been demonstrated and a socio-ethical framework proposed to encourage discussion and further research into the socio-ethical implications of the IoT with a focus on LBS and/or localization technologies. The proposed socio-ethical conceptual framework requires further elaboration and it is recommended that a thorough analysis, beyond information ethics, be conducted based on this paper which forms the basis for such future work. IoT by its very nature is subject to socio-ethical dilemmas because for the greater part, the human is removed from decision-making processes and is instead subject to a machine.

References

Abbas, R., Michael, K., Michael, M.G. & Aloudat, A.: Emerging Forms of Covert Surveillance Using GPS-Enabled Devices. Journal of Cases on Information Technology 13(2), 2011, 19-33.

Albrecht, K. & McIntyre, L.: Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move. Tomas Nelson 2005.

Albrecht, K. & Michael, K.: Connected: To Everyone and Everything. IEEE Technology and Society Magazine, Winter, 2013, 31-34.

Alder, G.S., Noel, T.W. & Ambrose, M.L.: Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust. Information & Management, 43, 2006, 894-903.

Aloudat, A. & Michael, K.: The Socio-Ethical Considerations Surrounding Government Mandated Location-Based Services During Emergencies: An Australian Case Study, in M. Quigley (ed.), ICT Ethics and Security in the 21st Century: New Developments and Applications. IGI Global, Hershey, PA, 2010, 1-26.

Aloudat, A. & Michael, K.: Toward the Regulation of Ubiquitous Mobile Government: A case Study on Location-Based Emergency Services in Australia. Electronic Commerce Research, 11(1), 2011, 31-74.

Andrejevic, M.: ISpy: Surveillance and Power in the Interactive Era. University Press of Kansas, Lawrence, 2007.

Arvidsson, A.: On the 'Pre-History of the Panoptic Sort': Mobility in Market Research. Surveillance & Society, 1(4), 2004, 456-474.

Ashton, K.: The "Internet of Things" Things. RFID Journal, 2009, www.rfidjournal.com/articles/pdf?4986

Barreras, A. & Mathur, A.: Chapter 18. Wireless Location Tracking, in K.R. Larsen and Z.A. Voronovich (eds.), Convenient or Invasive: The Information Age. Ethica Publishing, United States, 2007, 176-186.

Bauer, H.H., Barnes, S.J., Reichardt, T. & Neumann, M.M.: Driving the Consumer Acceptance of Mobile Marketing: A Theoretical Framework and Empirical Study. Journal of Electronic Commerce Research, 6(3), 2005, 181-192.

Beinat, E., Steenbruggen, J. & Wagtendonk, A.: Location Awareness 2020: A Foresight Study on Location and Sensor Services. Vrije Universiteit, Amsterdam, 2007, http://reference.kfupm.edu.sa/content/l/o/location_awareness_2020_2_108_86452.pdf

Bellavista, P., Küpper, A. & Helal, S.: Location-Based Services: Back to the Future. IEEE Pervasive Computing, 7(2), 2008, 85-89.

Bennett, C.J. & Regan, P.M.: Surveillance and Mobilities. Surveillance & Society, 1(4), 2004, 449-455.

Bentham, J. & Bowring, J.: The Works of Jeremy Bentham. Published under the Superintendence of His Executor, John Bowring, Volume IV, W. Tait, Edinburgh, 1843.

Blouin, D. An Intro to Internet of Things. 2014, www.xyht.com/spatial-itgis/intro-to-internet-of-things/

Boesen, J., Rode, J.A. & Mancini, C.: The Domestic Panopticon: Location Tracking in Families. UbiComp'10, Copenhagen, Denmark, 2010, pp. 65-74.

Böhm, A., Leiber, T. & Reufenheuser, B.: 'Trust and Transparency in Location-Based Services: Making Users Lose Their Fear of Big Brother. Proceedings Mobile HCI 2004 Workshop On Location Systems Privacy and Control, Glasgow, UK, 2004, 1-4.

Capurro, R.: Towards an Ontological Foundation of Information Ethics. Ethics and Information Technology, 8, 2006, 175-186.

Casal, C.R.: Impact of Location-Aware Services on the Privacy/Security Balance, Info: the Journal of Policy, Regulation and Strategy for Telecommunications. Information and Media, 6(2), 2004, 105-111.

Chellappa, R. & Sin, R.G.: Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management, 6, 2005, 181-202.

Chen, J.V., Ross, W. & Huang, S.F.: Privacy, Trust, and Justice Considerations for Location-Based Mobile Telecommunication Services. info, 10(4), 2008, 30-45.

Chen, J.V. & Ross, W.H.: The Managerial Decision to Implement Electronic Surveillance at Work. International Journal of Organizational Analysis, 13(3), 2005, 244-268.

Clarke, R.: Information Technology and Dataveillance. Communications of the ACM, 31(5), 1988, 498-512.

Clarke, R.: Profiling: A Hidden Challenge to the Regulation of Data Surveillance. 1993, http://www.roger-clarke.com/DV/PaperProfiling.html.

Clarke, R.: The Digital Persona and Its Application to Data Surveillance. 1994, http://www.roger-clarke.com/DV/DigPersona.html.

Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions of Terms. 1997, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Clarke, R.: Person Location and Person Tracking - Technologies, Risks and Policy Implications. Information Technology & People, 14(2), 2001b, 206-231.

Clarke, R.: Privacy as a Means of Engendering Trust in Cyberspace Commerce. The University of New South Wales Law Journal, 24(1), 2001c, 290-297.

Clarke, R.: While You Were Sleeping… Surveillance Technologies Arrived. Australian Quarterly, 73(1), 2001d, 10-14.

Clarke, R.: Privacy on the Move: The Impacts of Mobile Technologies on Consumers and Citizens. 2003b, http://www.anu.edu.au/people/Roger.Clarke/DV/MPrivacy.html.

Clarke, R.: Have We Learnt to Love Big Brother? Issues, 71, June, 2005, 9-13.

Clarke, R.: What's 'Privacy'? 2006, http://www.rogerclarke.com/DV/Privacy.html.

Clarke, R. Chapter 3. What 'Uberveillance' Is and What to Do About It, in K. Michael and M.G. Michael (eds.), The Second Workshop on the Social Implications of National Security, University of Wollongong, Wollongong, Australia, 2007a, 27-46.

Clarke, R.: Chapter 4. Appendix to What 'Uberveillance' Is and What to Do About It: Surveillance Vignettes, in K. Michael and M.G. Michael (eds.), The Second Workshop on the Social Implications of National Security, University of Wollongong, Wollongong, Australia, 2007b, 47-60.

Clarke, R.: Surveillance Vignettes Presentation. 2007c, http://www.rogerclarke.com/DV/SurvVign-071029.ppt.

Clarke, R.: Privacy Impact Assessment: Its Origins and Development. Computer Law & Security Review, 25(2), 2009, 123-135.

Clarke, R. & Wigan, M.: You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies. 2011, http://www.rogerclarke.com/DV/YAWYB-CWP.html.

Culnan, M.J. & Bies, R.J.: Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, 59(2), 2003, 323-342.

Davis, D.W. & Silver, B.D.: Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. American Journal of Political Science, 48(1), 2004, pp. 28-46.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V. & Serra, I.: Internet Users' Privacy Concerns and Attitudes Towards Government Surveillance – an Exploratory Study of Cross-Cultural Differences between Italy and the United States. 18th Bled eConference eIntegration in Action, Bled, Slovenia, 2005, 1-13.

Dobson, J.E. & Fisher, P.F. Geoslavery. IEEE Technology and Society Magazine, 22(1), 2003, 47-52.

Dobson, J.E. & Fisher, P.F. The Panopticon's Changing Geography. Geographical Review, 97(3), 2007, 307-323.

Dwyer, C., Hiltz, S.R. & Passerini, K.: Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, 2007, 1-12.

Elliot, G. & Phillips, N. Mobile Commerce and Wireless Computing Systems. Pearson Education Limited, Great Britain, 2004.

Ethics Subgroup IoT: Fact sheet- Ethics Subgroup IoT - Version 4.0, European Commission. 2013, 1-21, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1751&ei=5i7RVK-FHczYavKWgPgL&usg=AFQjCNG_VgeaUP_DIJVwSi-PIww3bC9Ug_w

Freescale Semiconductor Inc. and ARM Inc:, Whitepaper: What the Internet of Things (IoT) Needs to Become a Reality. 2014, 1-16, cache.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf

Floridi, L.: Information Ethics: On the Philosophical Foundation of Computer Ethics. Ethics and Information Technology, 1, 1999, 37-56.

Foucault, M. Discipline and Punish: The Birth of the Prison. Second Vintage Books Edition May 1995, Vintage Books: A Division of Random House Inc, New York, 1977.

Fusco, S.J., Michael, K., Aloudat, A. & Abbas, R.: Monitoring People Using Location-Based Social Networking and Its Negative Impact on Trust: An Exploratory Contextual Analysis of Five Types of "Friend" Relationships. IEEE Symposium on Technology and Society, Illinois, Chicago, 2011.

Fusco, S.J., Michael, K., Michael, M.G. & Abbas, R.: Exploring the Social Implications of Location Based Social Networking: An Inquiry into the Perceived Positive and Negative Impacts of Using LBSN between Friends. 9th International Conference on Mobile Business, Athens, Greece, IEEE, 2010, 230-237.

Gagnon, M., Jacob, J.D., Guta, A.: Treatment adherence redefined: a critical analysis of technotherapeutics. Nurs Inq. 20(1), 2013, 60-70.

Ganascia, J.G.: The Generalized Sousveillance Society. Social Science Information, 49(3), 2010, 489-507.

Gandy, O.H.: The Panoptic Sort: A Political Economy of Personal Information. Westview, Boulder, Colorado, 1993.

Giaglis, G.M., Kourouthanassis, P. & Tsamakos, A.: Chapter IV. Towards a Classification Framework for Mobile Location-Based Services, in B.E. Mennecke and T.J. Strader (eds.), Mobile Commerce: Technology, Theory and Applications. Idea Group Publishing, Hershey, US, 2003, 67-85.

Gould, J.B.: Playing with Fire: The Civil Liberties Implications of September 11th. Public Administration Review, 62, 2002, 74-79.

Jorns, O. & Quirchmayr, G.: Trust and Privacy in Location-Based Services. Elektrotechnik & Informationstechnik, 127(5), 2010, 151-155.

Junglas, I. & Spitzmüller, C.: A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services. Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, 1-10.

Kaasinen, E.: User Acceptance of Location-Aware Mobile Guides Based on Seven Field Studies. Behaviour & Information Technology, 24(1), 2003, 37-49.

Kaupins, G. & Minch, R.: Legal and Ethical Implications of Employee Location Monitoring. Proceedings of the 38th Hawaii International Conference on System Sciences. 2005, 1-10.

Kim, D.J., Ferrin, D.L. & Rao, H.R.: Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration. Information Systems Research, 20(2), 2009, 237-257.

King, L.: Information, Society and the Panopticon. The Western Journal of Graduate Research, 10(1), 2001, 40-50.

Kodl, J. & Lokay, M.: Human Identity, Human Identification and Human Security. Proceedings of the Conference on Security and Protection of Information, Idet Brno, Czech Republic, 2001, 129-138.

Kranenburg, R.V. and Bassi, A.: IoT Challenges, Communications in Mobile Computing. 1(9), 2012, 1-5.

Küpper, A. & Treu, G.: Next Generation Location-Based Services: Merging Positioning and Web 2.0., in L.T. Yang, A.B. Waluyo, J. Ma, L. Tan and B. Srinivasan (eds.), Mobile Intelligence. John Wiley & Sons Inc, Hoboken, New Jersey, 2010, 213-236.

Levin, A., Foster, M., West, B., Nicholson, M.J., Hernandez, T. & Cukier, W.: The Next Digital Divide: Online Social Network Privacy. Ryerson University, Ted Rogers School of Management, Privacy and Cyber Crime Institute, 2008, www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf.

Lewis, J.D. & Weigert, A.: Trust as a Social Reality. Social Forces, 63(4), 1985, 967-985.

Lyon, D.: The World Wide Web of Surveillance: The Internet and Off-World Power Flows. Information, Communication & Society, 1(1), 1998, 91-105.

Lyon, D.: Surveillance Society: Monitoring Everyday Life. Open University Press, Phildelphia, PA, 2001.

Lyon, D.: Surveillance Studies: An Overview. Polity, Cambridge, 2007.

Macquarie Dictionary.: 'Uberveillance', in S. Butler, Fifth Edition of the Macquarie Dictionary, Australia's National Dictionary. Sydney University, 2009, 1094.

Mann, S.: Sousveillance and Cyborglogs: A 30-Year Empirical Voyage through Ethical, Legal, and Policy Issues. Presence, 14(6), 2005, 625-646.

Mann, S., Nolan, J. & Wellman, B.: Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance & Society, 1(3), 2003, 331-355.

Mathiesen, K.: What is Information Ethics? Computers and Society, 32(8), 2004, 1-11.

Mattern, F. and Floerkemeier, K.: From the Internet of Computers to the Internet of Things, in Sachs, K., Petrov, I. & Guerrero, P. (eds.), From Active Data Management to Event-Based Systems and More. Springer-Verlag Berlin Heidelberg, 2010, 242-259.

Marx, G.T. & Steeves, V.: From the Beginning: Children as Subjects and Agents of Surveillance. Surveillance & Society, 7(3/4), 2010, 192-230.

Mayer, R.C., Davis, J.H. & Schoorman, F.D.: An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 1995, 709-734.

McKnight, D.H. & Chervany, N.L.: What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce, 6(2), 2001, 35-59.

Metzger, M.J.: Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. Journal of Computer-Mediated Communication, 9(4), 2004.

Michael, K. & Clarke, R.: Location and Tracking of Mobile Devices: Überveillance Stalks the Streets. Computer Law and Security Review, 29(2), 2013, 216-228.

Michael, K., McNamee, A. & Michael, M.G.: The Emerging Ethics of Humancentric GPS Tracking and Monitoring. International Conference on Mobile Business, Copenhagen, Denmark, IEEE Computer Society, 2006a, 1-10.

Michael, K., McNamee, A., Michael, M.G., and Tootell, H.: Location-Based Intelligence – Modeling Behavior in Humans using GPS. IEEE International Symposium on Technology and Society, 2006b.

Michael, K., Stroh, B., Berry, O., Muhlbauer, A. & Nicholls, T.: The Avian Flu Tracker - a Location Service Proof of Concept. Recent Advances in Security Technology, Australian Homeland Security Research Centre, 2006, 1-11.

Michael, K. and Michael, M.G.: Australia and the New Technologies: Towards Evidence Based Policy in Public Administration (1 ed). Wollongong, Australia: University of Wollongong, 2008, Available at: http://works.bepress.com/kmichael/93

Michael, K. & Michael, M.G.: Microchipping People: The Rise of the Electrophorus. Quadrant, 49(3), 2005, 22-33.

Michael, K. and Michael, M.G.: From Dataveillance to Überveillance (Uberveillance) and the Realpolitik of the Transparent Society (1 ed). Wollongong: University of Wollongong, 2007. Available at: http://works.bepress.com/kmichael/51.

Michael, K. & Michael, M.G.: Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants. IGI Global, Hershey, PA, 2009.

Michael, K. & Michael, M.G.: The Social and Behavioral Implications of Location-Based Services. Journal of Location-Based Services, 5(3/4), 2011, 1-15, http://works.bepress.com/kmichael/246.

Michael, K. & Michael, M.G.: Sousveillance and Point of View Technologies in Law Enforcement: An Overview, in The Sixth Workshop on the Social Implications of National Security: Sousveillance and Point of View Technologies in Law Enforcement, University of Sydney, NSW, Australia, Feb. 2012.

Michael, K., Roussos, G., Huang, G.Q., Gadh, R., Chattopadhyay, A., Prabhu, S. and Chu, P.: Planetary-scale RFID Services in an Age of Uberveillance. Proceedings of the IEEE, 98.9, 2010, 1663-1671.

Michael, M.G. and Michael, K.: National Security: The Social Implications of the Politics of Transparency. Prometheus, 24(4), 2006, 359-364.

Michael, M.G. & Michael, K. Towards a State of Uberveillance. IEEE Technology and Society Magazine, 29(2), 2010, 9-16.

Michael, M.G. & Michael, K. (eds): Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies. Hershey, PA, IGI Global, 2013.

O'Connor, P.J. & Godar, S.H.: Chapter XIII. We Know Where You Are: The Ethics of LBS Advertising, in B.E. Mennecke and T.J. Strader (eds.), Mobile Commerce: Technology, Theory and Applications, Idea Group Publishing, Hershey, US, 2003, 245-261.

Orwell, G.: Nineteen Eighty Four. McPherson Printing Group, Maryborough, Victoria, 1949.

Oxford Dictionary: Control, Oxford University Press, 2012a http://oxforddictionaries.com/definition/control?q=control.

Oxford Dictionary: Trust, Oxford University Press, 2012b, http://oxforddictionaries.com/definition/trust?q=trust.

Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 2003, 69-103.

Perusco, L. & Michael, K.: Humancentric Applications of Precise Location Based Services, in IEEE International Conference on e-Business Engineering, Beijing, China, IEEE Computer Society, 2005, 409-418.

Perusco, L. & Michael, K.: Control, Trust, Privacy, and Security: Evaluating Location-Based Services. IEEE Technology and Society Magazine, 26(1), 2007, 4-16.

Perusco, L., Michael, K. & Michael, M.G.: Location-Based Services and the Privacy-Security Dichotomy, in Proceedings of the Third International Conference on Mobile Computing and Ubiquitous Networking, London, UK, Information Processing Society of Japan, 2006, 91-98.

Quinn, M.J.: Ethics for the Information Age. Second Edition, Pearson/Addison-Wesley, Boston, 2006.

Renegar, B., Michael, K. & Michael, M.G.: Privacy, Value and Control Issues in Four Mobile Business Applications, in 7th International Conference on Mobile Business (ICMB2008), Barcelona, Spain, IEEE Computer Society, 2008, 30-40.

Rozenfeld, M.: The Value of Privacy: Safeguarding your information in the age of the Internet of Everything, The Institute: the IEEE News Source, 2014, http://theinstitute.ieee.org/technology-focus/technology-topic/the-value-of-privacy.

Rummel, R.J.: Death by Government. Transaction Publishers, New Brunswick, New Jersey, 1997.

Sanquist, T.F., Mahy, H. & Morris, F.: An Exploratory Risk Perception Study of Attitudes toward Homeland Security Systems. Risk Analysis, 28(4), 2008, 1125-1133.

Schoorman, F.D., Mayer, R.C. & Davis, J.H.: An Integrative Model of Organizational Trust: Past, Present, and Future. Academy of Management Review, 32(2), 2007, 344-354.

Shay, L.A., Conti, G., Larkin, D., Nelson, J.: A framework for analysis of quotidian exposure in an instrumented world. IEEE International Carnahan Conference on Security Technology (ICCST), 2012, 126-134.

Siau, K. & Shen, Z.: Building Customer Trust in Mobile Commerce. Communications of the ACM, 46(4), 2003, 91-94.

Solove, D.: Digital Dossiers and the Dissipation of Fourth Amendment Privacy. Southern California Law Review, 75, 2002, 1083-1168.

Solove, D.: The Digital Person: Technology and Privacy in the Information Age. New York University Press, New York, 2004.

Tavani, H.T.: Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology. John Wiley, Hoboken, N.J., 2007.

Valacich, J.S.: Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments. Business, Washington State University, 2003, 1-2.

van Ooijen, C. & Nouwt, S.: Power and Privacy: The Use of LBS in Dutch Public Administration, in B. van Loenen, J.W.J. Besemer and J.A. Zevenbergen (eds.), Sdi Convergence. Research, Emerging Trends, and Critical Assessment, Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009, 75-88.

Wakunuma, K.J. and Stahl, B.C.: Tomorrow's Ethics and Today's Response: An Investigation into The Ways Information Systems Professionals Perceive and Address Emerging Ethical Issues. Inf Syst Front, 16, 2014, 383–397.

Weckert, J.: Trust and Monitoring in the Workplace. IEEE International Symposium on Technology and Society, 2000. University as a Bridge from Technology to Society, 2000, 245-250.

Wigan, M. & Clarke, R.: Social Impacts of Transport Surveillance. Prometheus, 24(4), 2006, 389-403.

Xu, H. & Teo, H.H.: Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective. Twenty-Fifth International Conference on Information Systems, 2004, 793-806.

Xu, H., Teo, H.H. & Tan, B.C.Y.: Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk. Twenty-Sixth International Conference on Information Systems, 2005, 897-910.

Yan, Z. & Holtmanns, S.: Trust Modeling and Management: From Social Trust to Digital Trust, in R. Subramanian (ed.), Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. IGI Global, 2008, 290-323.

Yeh, Y.S. & Li, Y.M.: Building Trust in M-Commerce: Contributions from Quality and Satisfaction. Online Information Review, 33(6), 2009, 1066-1086.