



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2008

A research note on ethics in the emerging age of Überveillance

M. G. Michael

University of Wollongong, mgm@uow.edu.au

Sarah Jean Fusco

University of Wollongong, sjf462@uow.edu.au

Katina Michael

University of Wollongong, katina@uow.edu.au

Publication Details

Michael, M. G., Fusco, S. Jean. & Michael, K. (2008). A research note on ethics in the emerging age of überveillance. *Computer Communications*, 31 (6), 1192-1199.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library:
research-pubs@uow.edu.au

A research note on ethics in the emerging age of Überveillance

Abstract

Advanced location-based services (A-LBS) for human-centric tracking and monitoring are now emerging as operators and service providers begin to leverage their existing infrastructure and invest in new technologies, toward increasingly innovative location application solutions. We can now point to human-centric tracking and monitoring services where the person (i.e. subject) has become an active node in the network. For example, in health applications through the use of embedded technologies such as radio-frequency identification (RFID) or in campus applications through the use of electronic monitoring techniques in the form of global positioning systems (GPS). These technologies, for the greater part, have been introduced into society at large, without the commensurate assessment of what they will mean in terms of socio-ethical implications. Of particular concern is the potential for these innovative solutions to be applied in government-to-citizen mandated services, increasing the ability of the state to collect targeted data and conduct covert surveillance on any given individual, described herein as überveillance. This paper aims to define, describe, and interpret the current socio-ethical landscape of advanced location-based services for humans in order to promote discourse among researchers and practitioners to better direct telecommunications policy.

Keywords

Location-based services, radio frequency identification, global positioning system, socio-ethics, überveillance, uberveillance

Disciplines

Physical Sciences and Mathematics

Publication Details

Michael, M. G., Fusco, S. Jean. & Michael, K. (2008). A research note on ethics in the emerging age of überveillance. *Computer Communications*, 31 (6), 1192-1199.

Title:

A Research Note on Ethics in the Emerging Age of Überveillance

Author Names and Affiliation:

M.G. Michael, Sarah Jean Fusco, Katina Michael

School of Information Systems and Technology, Faculty of Informatics, University of Wollongong, NSW 2522 Australia

{mgm, sjf462, katina}@uow.edu.au

Corresponding Author:

Katina Michael

P: 61242213937

F: 61242214045

katina@uow.edu.au

PO Box U184, University of Wollongong, NSW Australia 2500

Abstract:

Advanced location-based services (A-LBS) for human-centric tracking and monitoring are now emerging as operators and service providers begin to leverage their existing infrastructure and invest in new technologies, toward increasingly innovative location application solutions. We can now point to human-centric tracking and monitoring services where the person (i.e. subject) has become an active node in the network. For example, in health applications through the use of embedded technologies such as radio-frequency identification (RFID) or in campus applications through the use of electronic monitoring techniques in the form of global positioning systems (GPS). These technologies, for the greater part, have been introduced into society at large, without the commensurate assessment of what they will mean in terms of socio-ethical implications. Of particular concern is the potential for these innovative solutions to be applied in government-to-citizen mandated services, increasing the ability of the state to collect targeted data and conduct covert surveillance on any given individual, described herein as überveillance. This paper aims to define, describe, and interpret the current socio-ethical landscape of advanced location-based services for humans in order to promote discourse among researchers and practitioners to better direct telecommunications policy.

Keywords:

Location-based services, radio frequency identification, global positioning system, socio-ethics, überveillance

1 Introduction

Since their inception, location positioning technologies have significantly improved, in terms of their accuracy, portability and affordability. For the first time we are witnessing the diffusion of sophisticated carrier-grade location-based service (LBS) applications for humancentric tracking and monitoring. The full potential for LBS is only now being realised. Commercial LBS applications are currently being used for care, control, and convenience, albeit for niche markets. For example, humancentric tracking and monitoring devices can be used to enable families to track and monitor their loved ones, or in the case of doctors to remotely supervise their patients' vital signs. From a business, government, and emergency sector view, humancentric tracking and monitoring applications include enterprise collaboration, ePassports, Enhanced 911 (E-911), the monitoring of parolees, as well as tracking systems that can create a breadcrumb of a subject's movements for law enforcement purposes. These currently available LBS solutions coupled with the increasing rate of technological progress and the readiness of society to embrace the new technology, reveal the ubiquitous nature of humancentric LBS. These solutions can be considered advanced location-based services (A-LBS), not only because of the technology being utilised but the functionality of the given service. Only modest research however, has been dedicated to establishing the potential threat or risk of these emerging applications upon crucial aspects such as the privacy encroachment on society.

2 Background

If we are to accept the position of Davis [1], "technology has no conscience of its own." LBS value chain stakeholders involved in the complex innovation process must then equip themselves with the knowledge and tools to understand the current and potential socio-ethical implications. What is required is a technological assessment, which is the process by which we "extend a voice questioning the chaotic progression of technology without analysis" [1]. It is one thing to invent, to create, to develop, and another thing altogether to see a value or positive contribution to our lives through the adoption of a given technology. For the time being, the all critical component of context in LBS innovation for the greater part has been largely ignored. For instance, E-911 LBS pinpointing services helping to save lives during emergency response have not been conceptualised any differently to the 'on-demand' trailing of minors by parents or guardians. Whilst some discussion of the socio-ethical implications of humancentric tracking and monitoring has begun, it is quite clearly in its infancy.

The purpose of this paper is to provide a view of the current socio-ethical landscape of location-based services for humancentric tracking and monitoring. This is achieved by performing a content analysis of the current academic literature in the related area. By reviewing the landscape we are able to first understand the currently explored social and ethical dimensions; and second, to reveal whether there is a gap in the existing technological assessment. Understanding the socio-ethical implications is critically important to the long-term development and sustainability of A-LBS. It will facilitate and guide the formation of policy and legislation which will regulate the use of the technology so that it can benefit and contribute to society without unnecessarily complicating lives and infringing upon the individual's rights and freedoms.

2.1 Definitions

There are five terms that need to be defined in the context of this paper before we are able to progress: (i) humancentric LBS technology, (ii) humancentric tracking, (iii) humancentric monitoring, (iv) ethics, and (v) socio-ethics. *Humancentric LBS technology* is any technology that can be utilized to determine remotely the position of a person. Included in this definition are location-based technologies that are implantable, wearable and luggable. For example, an implantable RFID chip, a wearable active smart card

badge, or a portable personal digital assistant with an onboard GPS receiver is considered humancentric LBS. Once a consumer or member of society subscribes themselves to a location service or is mandated to use one, the location technology allows for the tracking of the human, to a varying degree of detail, dependent on the limitations of the device they are carrying and the provisioned network infrastructure supporting the service.

Humancentric tracking is therefore the act of following someone or something, in order to find that individual and to understand their pattern of movement over a period of time, or note their course for a particular purpose. Tracking and monitoring although often used synonymously in the literature are different. *Humancentric monitoring* is the discrete observation or the continuous real-time observation of a subject, examining, inspecting or scrutinizing their progress or their given state over a period of time for the purposes of systematic review and revision. Tracking can therefore be considered voluntary and approximate with the purpose to locate an individual at a given time (e.g. Buddy-Finder service), while monitoring can be considered something which is enforced, constant and precise (e.g. parolee electronic monitoring). Tracking is about knowing a person's particular course, whereas monitoring is about alerting a system or person that something is wrong or someone is off course or outside a given set of parameters. Monitoring generally implies tracking by default and is more about noting exceptions, while tracking is about providing a chronicle of movement.

Choice, consent, the ability to opt-in or opt-out of a location-based service are paramount in the product/process development discussion, despite the fact that much has yet to be recorded on these important matters. A great deal of the debate which is yet to happen will revolve around ethics. *Ethics* can be defined as the moral principles that govern a person's behavior or conduct in a given instance, activity or scenario. It then follows that *socio-ethics* are the moral principles which govern a particular society at large.

3 Qualitative Content Analysis

This study used a content analysis methodology to develop a view of the current socio-ethical implications of humancentric LBS. A qualitative content analysis can be defined as an objective and systematic technique of making inferences from data [2]. By performing a qualitative content analysis on the academic articles in this area of study, concepts and interrelationships are revealed at a theoretical level providing a view of the landscape of socio-ethical implications of humancentric LBS. The three stages of this content analysis included: (i) the design, (ii) implementation, and (iii) reporting.

3.1 Design

The collection of data involved defining a search strategy and outlined the restrictions on the data to be collected. The search method established had two tiers. First, the terms "location-based services", "radio-frequency identification", and "global positioning system" were searched, and secondly the results were refined to identify articles which contained the word "ethics". This method was chosen to be inclusive of literature, so that as many relevant and related articles on "LBS and ethics" would be included in the sample.

The guide for collecting articles was as follows. First, the literature search was limited to the following online databases: ACM Digital Library, Cambridge Journals Online, Compendex, Thompson Computer Datagae, Expanded Academic ASAP, IEEE Xplorer, Springerlink, Proquest 5000, Proquest Computing, Science Direct, Synergy, Taylor and Francis, Web of Knowledge. The study included electronic articles available as of January 2007. Second, the articles retained had to be academic research, review, case or application-based papers. The focus was on using only substantive academic research so emotive tabloid-type media articles were not included in the search process. Finally, only electronically formatted articles were retained for the purposes of content processing using the *Leximancer* content analysis application [3].

The analytic technique chosen utilizes contingency analysis, which “aims to infer the network of sources associations from the pattern of co-occurrences of symbolic images” [2]. *Leximancer* performs this task and produces concept maps and ranked lists which can then be used to identify the prominent concepts enunciated by the literature helping to understand the interrelationships between them. A high level of reliability and validity is provided by using *Leximancer* to perform the content analysis. *Leximancer*, being software, does not suffer from the human condition of exhaustion and offers a high level of coding stability through “the automated and deterministic machine learning phase [which is] ... highly consistent no matter how many times a corpus is processed and reprocessed by the application” [4]. Its major strength is reproducibility, and an enhanced improved reliability. The software program also helps to address the problem of identification and hence improves validity [5].

3.2 Implement

The number of relevant academic articles found in the above-mentioned online databases was sixty-two. The total number of articles pertaining specifically to ethics and humancentric tracking and monitoring were only twenty-eight. In order to ensure that the corpus of articles was representative of the current literature the reference list of each article was exhaustively examined. As a result only seven additional articles were added to the overall count, taking the total number of articles analyzed to thirty-five. The data was then modified where required, ready for computerized content analysis. *Leximancer* was then used to analyze the content of the articles. The following terms were merged in *Leximancer* to avoid redundancy of concepts: LBS included “LBS” and “location based service”; RFID included “RFID” and “radio frequency identification”; GPS included “GPS” and “Global Positioning System”; Law included “Legislation”, “Law” and “Legal”.

3.3 Report

Leximancer produces the results of the qualitative content analysis with a graphical concept map and a tabular list of ranked concepts. Before observing and interpreting the results produced from the content analysis it is important to note the size of the corpus of articles analyzed. Only a small number of articles retrieved, reveals the limited amount of academic engagement in this area. Plainly, LBS and socio-ethical issues are under explored. The study can therefore only be granted research note status, based on the

preliminary evidence available to the researchers. We thus present an emerging LBS socio-ethical framework.

Diagram 1 shows the study's concept map with "people", "monitoring", and "technology" being the focal points in the current literature. Leximancer's ranked concept list for the study included: technology, information, privacy, location, RFID, people, system, devices, applications, tracking, tags, LBS, data, individual, services, security, monitoring, GPS, time, case, control, issues, should, personal, potential, trust, access, future, identification, provide, available, number, user, work, current, mobile, surveillance, research, government, reader, children, public, chip, social, law, network, consumers, include, enforcement, society, home, phone, computer. By reviewing the concept maps and ranked list provided by Leximancer it logically emerged that concepts fell broadly into three categories: actors, social issues, and technologies (Table 1). Other significant concepts which are overarching in terms of their applicability to the categories listed include "law", "potential", "future", and "research", indicating the underlying need for a socio-ethical framework to be developed and utilized for A-LBS development.

4 Findings

The content analysis results reveal the dominant concepts emerging from the academic research on the socio-ethical implications of humancentric LBS. The analysis also shows the relationship between these different concepts. By analyzing these concepts and their associations a socio-ethical framework has been developed. The content analysis reveals that the literature identifies relationships between actors in society in terms of "privacy", "security", "control" and "trust". Overlaying these relationships and implications are the concepts of "technology", "potential", and "future". When these concepts are explored deeper using Leximancer it is evidenced that the limitations of LBS technology (i.e. fallibility) and its potential applications, as well as potential advancement in the future, compound upon and amplify the already present socio-ethical concerns. The current technological and legislative efforts which aim to alleviate the socio-ethical implications of humancentric LBS are also addressed by the literature. This paper will now explore the relationships between actors, social issues, future and potential uses of LBS technology, and the legislative and technological efforts that ensue. A more detailed view of the current socio-ethical landscape of humancentric location-based services is presented. Diagram 2 illustrates these complex relationships.

4.1 Actors and Relationships

The *individual* in diagram 2 is defined as a citizen at home or roaming a public space, an employee at work or on-site, or a consumer in society (local or international). The actors surrounding the individual in diagram 2 utilize location services to track and/or monitor the "individual" in a variety of contexts. The lines connecting the actors in the diagram represent a significant relationship that provides a vehicle for observing LBS applications for humancentric tracking and monitoring and their resultant implications. Before discussing the implications in terms of the social issues, this paper will review the present and perceived applications of LBS technologies provided by the literature in terms of the relationships between the actors.

4.1.1 Employee and Employer

Location technologies can be used to allow employers to monitor the location of employees in order to improve productivity [6]. In the latter part of 2007 there were a number of cases reported which stipulated that the U.S. government had terminated an employee's contract based on data collected covertly using the GPS chipset in the government-owned mobile handset carried by the employee. Most of these cases have focused on the physical location of the employee, i.e. that employees were claiming financial remuneration for hours not physically worked at the office. Trucking unions in the United States are even questioning the use of GPS receivers on heavy vehicles as a form of covert employer-employee monitoring.

4.1.2 Citizen and Government

Some governments, like the United States, have mandated the use of LBS technologies by wireless operators to assist in emergency services to locate individuals, such as the Enhanced 911 (E-911) service. E-911 has the potential to save lives, however it also has the "potential to collect, store and analyze every place individuals go with their cell phone" [7]. Another example of a government mandated initiative to track and monitor citizens is the ePassport. The ePassport has been implemented to provide a secure means of identification. However by utilizing the RFID technology it also allows for the tracking of individuals while they are physically carrying their passport [8].

4.1.3 Patient and Doctor

Xiao, Shen, Sun and Cai [9] propose two applications for human-centric LBS in the area of telemedicine. The first is that doctors, nurses and patients be RFID tagged to ensure an optimal level of care be maintained in a hospital so that the supply of staff and the demand of patients is at equilibrium. The second application is the ability to remotely monitor the elderly at home and to assist carers with providing quality care. LBS technology could thus be used in a variety of healthcare applications- in a hospital, at home, on the move (in an ambulance), or in response to a disaster. The purpose of such an application is to provide a "real time patient monitoring system that can use smart sensors to collect patients vital signs so that medical specialists can perform remote diagnosis anywhere and anytime" [9]. A second academic article suggests that LBS can be used for the purpose of identifying individuals medical records and to couple this information with a biomedical device that can "detect, record and transmit information regarding physiological change or the presence of various chemicals or biological materials in the environment" [10]. Further to detecting, recording and transmitting this information, it is suggested that the LBS technology be combined with a therapeutic device which provides treatment in response.

4.1.4 Individual and Family

LBS technologies are currently utilized to monitor families. For example, at Wannado City Theme Park, RFID wristbands are provided to all visitors so that they can locate their families using touch screen kiosks available throughout the park [11]. This technology can be extended such that in the future "tags will be embedded into children to advise parents of their locations" [10]. It is also suggested that schools will be able to locate their students if they are absent from class [12]. There are also currently available

commercial products such as the VeriChip which is marketed as a means of identifying kidnapped victims who are drugged, unconscious or dead [10]. WherifyWireless is another company who has invested in a number of different types of global location devices specifically for parents or guardians of children, and carers of the elderly.

4.1.5 Consumer and Corporation

The use of RFID in the retail sector is attractive as it claims to reduce costs, improve services and enhance convenience. This technology can also be used to track and monitor consumers [11]. RFID devices may also be used for financial services in the future, removing the need for people to carry cash or credit cards. This will also enable the user to be tracked and monitored, either because they are carrying the RFID device or because it is implanted in them [10]. Mobile location advertising is another potential enterprise location service targeted at consumers based on their proximity to a store, personal profile, and historical buying behavior.

4.1.6 Individual and Society

There are many ways in which LBS technologies can be utilized by society in general. The purpose of such applications will vary from paternal or investigative objectives to curious or perverted aims. For example, basic Friend-Finder applications can be used to alert friends or persons of interest who are in proximity of one another. However, some applications such as E-911 can be misused by unauthorized persons to obtain location information [7]. For the present, IP-based location technologies currently pose the greatest potential risks to society.

4.2 Social Issues

From the content analysis results it is shown that the academic literature bases its discussion of the socio-ethical implications of LBS around four broad social issues. These are the universal, but sometimes differently understood and applied concepts of (i) *trust*, (ii) *control*, (iii) *security*, and (iv) *privacy*.

4.2.1 Trust

Trust is defined as the ability to “to have faith or confidence; to place reliance; to confide” [13]. In the context of this paper it is recognized that the essence of trust is the “lack of complete knowledge” and therefore “an absence of surveillance and a degree of ignorance is necessary for trustworthiness to be developed and demonstrated” [14]. Trust is closely allied to autonomy, independence and freedom. The content analysis has revealed the importance of trust to the functioning of society and the potential implications that humancentric LBS will have on trust between people. Trust is seen as a vitally important part of human existence [15]. It is acknowledged that it is “difficult to have a well-functioning and happy community or workplace without a high level of trust. It is also difficult to have a high level of self-respect without the trust of others, and lack of trust in others indicates lack of respect for others” [16]. Furthermore when there is no trust there is “no bonding, no giving and no risk taking” [15]. Trust is therefore an important aspect of relationships, and the maintenance and building of trust enables meaningful connections between human beings. Advanced humancentric LBS applications however pose a threat to the maintenance and propagation of trust.

Trust involves the “lack of complete knowledge” [14] and therefore humancentric LBS undermine trust by providing an unobtrusive means of obtaining location knowledge. What results is a transferal of trust, from trust in an individual to trust in technology. The undermining or removal of trust from human relationships poses a significant threat to the individual’s ability to form meaningful connections to other human beings, and without these connections society will “literally fall apart” over time [15]. The academic literature provides scenarios which reveal that the application of LBS for humancentric tracking and monitoring can erode trust and cause relationships to degrade.

LBS technologies, “though designed to protect the safety of a loved one may end up undermining communication and trust between family members” [14]. This technology will replace trust in the workplace with surveillance [8], although to a degree this has already happened since the proliferation of inexpensive closed circuit television (CCTV). The tracking and monitoring of employees can in some circumstances be economically and strategically justified, however regardless of any such justification there are two overriding concerns which arise. First, since respect in general implies trust, then when trust is lost through monitoring so too is respect. Second, workplace monitoring may result in a workplace with low trust that will then require more surveillance due to the lack of trust in the workplace, which will then erode the trust even further [16].

The impact of LBS on trust and therefore on human relationships and society is not limited to the examples above. The relationship of husband and wife can be eroded [17], so too can LBS technologies destroy consumer trust in the commercial sphere [18]. In fact in any situation in which humancentric LBS are utilized, the trust and hence relationship between actors in society could potentially be damaged.

4.2.2 Control

Control is the ability “to exercise restraint or direction upon the free action of; to hold sway over, exercise power or authority over; to dominate [or], command” others [13]. The significant issue is “who has control and who does not” [19]. The distribution of control (i.e. power) impacts the ability of humans to operate as autonomous individuals, potentially causing humans to feel desperate, helpless, and powerless [20]. The application of LBS for humancentric tracking and monitoring has an “overarching element of control” [15]. A clear example of utilizing LBS technologies to exert control is provided by Dobson and Fisher's account of “Geoslavery”. Geoslavery is defined as “the practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave” [21]. This raises significant human rights issues as those with the lack of knowledge and awareness can be coerced, deceived or persuaded into geoslavery. LBS can be used for geoslavery in any of the relationships identified. It is not only the threat of government enslaving the citizens creating an Orwellian (or even a neo-Stalinist) society but also that families, corporations, employers and other individuals in society can utilize LBS for similar purposes.

4.2.3 Security

Security is “the condition of being protected from or not exposed to danger” [13]. LBS can be used to ensure security. For example, GPS devices are used by law enforcement in order to make “police more efficient in the war against crime” [22]. In addition, law enforcement authorities who are granted warrants to monitor suspected criminals, have utilized very small GPS devices to track vehicles, in order to provide location-specific evidence in a court of law. Glasser, Goodman and Norman [12] also note that embedding chips into personal documents such as passports can assist law enforcement and homeland security officials. These applications theoretically are more secure if implanted under the skin enabling, for example, victims of kidnapping to be located. However as *technology giveth, technology taketh away*. These technologies can also present a threat to security as prying individuals or terrorists can obtain the location information in the same manner as law enforcement agencies. Vance Lockton [23] points out that, “when someone steals a car the first thing they disarm is the location device, kidnappers will obviously know that this technology exists... since the chips are always injected in the same location we are left with a grisly scenario in which identification can be removed from their owners... should banks or government agencies use chips for access to high security areas these chips will become very valuable... while it may be difficult to steal this form of identification it is certainly not impossible”.

4.2.4 Privacy

Privacy is the “right or entitlement to solitude, autonomy and individuality such that with it we are able to go where we please, love whom we want... live the kind of life we want” [12]. When our privacy is impinged “we believe we have been both wronged and harmed” [12]. The content analysis showed that LBS technologies pose a threat to our privacy in the way the information is collected, retained, used and disclosed. LBS have the potential to track individuals without their knowledge [24] and therefore the manner in which information is collected, retained, used and disclosed brings about privacy issues. For example, there is currently the ability to skim information from ePassports at airports obtaining such details as the passport holder’s name, address and date of birth. This method can also be used by police to identify people at a rally, and this highlights that the technology can be used for hitherto unintended purposes. The passport holder does not have the ability to control the disclosure of his or her own personal information [23].

If the privacy factors of LBS are not addressed then we may face a “[d]omesday scenario in which corporate and government interest can pervasively track individuals- paving the way for a techno totalitarian state in which each persons movements, associations, and casual acquaintances are carefully monitored and recorded” [24]. It is important to note however that while privacy is important, in situations of emergency the perceived intrusion upon privacy is lower [25]. Furthermore in order to achieve a designated level of security we must forgo some privacy [10]. As LBS technology advances and becomes more and more pervasive, it will become increasingly difficult to classify what constitutes a public or private space.

4.3 Technology

Overlaying the preceding discussion of relationships and social issues are the limitations of technology and its future application, as well as technical potential. As service providers attempt to overcome limitations in given technologies, they have introduced novel services based on dual modes of operation, such as GPS and cellular mobile. Handset manufacturers, foreseeing the future possibilities of LBS have already tested the market with advanced smart phones or PDAs that contain the traditional cellular mobile function with an embedded GPS chipset and onboard RFID reader at the base of the unit.

In diagram 2, technological concerns surround the actors and social issues. The potential of LBS technology to evolve into something with grave power is explored by Adam Stone [26] in his article “The Dark Side of Pervasive Computing.” Stone poses several scenarios based around evolved forms of LBS technologies providing insight into a possible future. For example, Stone proposes that humanity will eventually phase out the need for their own physical bodies as they continually endeavor to make tasks easier to perform. Stone [26] also mentions that these technologies may one day be used to enhance human beings, enabling us to jump higher and even read people’s thoughts. These proposals are comparable to science fiction, however the technology to perform such bio-engineering marvels is looming closely and we must endeavor to identify the potential applications of the technology and its socio-ethical implications before it is fully unleashed. Jacques Ellul [27] forewarned of such ominous happenings as far back as 1964.

4.4 Current Technical and Legislative Measures

The literature also looks at the current technical solutions and legislative framework for LBS. A constant theme among the articles is that there is a need for legislation and social awareness. Several technical solutions pertaining to technologies like RFID have been proposed including tag killing, blocker tag, encryption and antenna-energy analysis [24]. However there are two problems with technical solutions. First, that in a time of emergency any technical protection may be deliberately unobserved. And second, that no technical safeguards are 100% fail proof- it is only a matter of time until someone devises a way to break it [23].

There is evidently a lag in policy and legislation addressing LBS [26]. Despite that LBS are still considered a relatively emerging technology it has already been shown through case law in the United States, that there is a lack of legislation in place to assist in their operation. Smith identifies that there are problems with the current regulatory mechanisms to govern the use of Enhanced 911 and that legislative amendments are required [7]. Eva Maria Dowdell reviewed court cases involving the use of GPS for humancentric tracking and monitoring revealing inconsistencies and anomalies in decisions and in the manner in which courts have interpreted evidence. Dowdell [22] explains that the reason for this is that courts are “shoehorning GPS into established technical doctrines”. This reveals that amendments are needed to legislation to address the unique characteristics of LBS technologies. Many of the authors already cited [10, 17, 23] concur with Dowdell.

5 The Emerging Age of Überveillance

The socio-ethical issues raised in this paper can be described as issues in an age we have described as *überveillance*. *Überveillance* is an emerging concept. In the full sense of both its application and power it is not yet arrived [28]. For some time Roger Clarke's [29] *dataveillance* has been prevalent: the "systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons". *Überveillance* is an *above* and *beyond*, an exaggerated, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on" but "always with you" (it is ubiquitous) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of invasive surveillance is that omnipresence in the 'material' world will not always equate with omniscience, hence the real concern for *misinformation*, *misinterpretation*, and *information manipulation*.

Überveillance takes that which was "static" or "discrete" in the *dataveillance* world, and makes it "constant" and "embedded". Consider it not only "automatic" and to do with "identification" but also about "location"- that is, the ability to automatically locate and identify- in essence the ability to perform automatic location identification (ALI). It has to do with the fundamental "who" (ID), "where" (location), "when" (time) questions in an attempt to derive "why" (motivation), "what" (result), and even "how" (method/plan/thought). *Überveillance* can be a predictive mechanism for one's expected behavior, traits, characteristics, likes or dislikes; or it can be based on historical fact, or something in between. The inherent problem with *überveillance* is that facts do not always add up to truth (i.e. as in the case of an exclusive disjunction $T+T=F$), and predictions based on intelligence are not always correct. *Überveillance* is more than closed circuit television (CCTV) feeds, or cross-agency databases linked to national identity cards, or biometrics and ePassports used for international travel. *Überveillance* is the sum total of all these types of surveillance and the deliberate integration of an individual's personal data for the continuous tracking and monitoring of identity and location in real time [30, 31, 32, 33, 34, 35].

5.1 The Need for Public Debate and Discourse

As we prepare for the introduction of fully fledged advanced humancentric location-based applications we need to be mindful of the potential socio-ethical changes that will occur as a result. These "changes" will also include new perspectives to traditional metaphysics as embedded in the flesh technologies challenge us to potentially "updated" definitions of *identity* and *self-consciousness* for instance. For the present, technological advancements in this space of research and investigation always seem to take precedence over discussion of the potential detrimental effects to individuals or society at large. There need to be adequate and applicable safeguards 'built-in' if we are to innovate smartly; we cannot hope to 'bolt-on' band-aid solutions on the off chance that things might go wrong. And things normally do go wrong.

6 Conclusion

The content analysis results provide a preliminary understanding of the socio-ethical implications of LBS for humancentric tracking and monitoring. Further research should be conducted to provide a comprehensive landscape of the socio-ethics of humancentric LBS, which can then be utilized to create legislation, policies and social awareness. The

application of LBS for humancentric tracking and monitoring is threatening to become ubiquitous in society as the technology rapidly evolves. The pervasive nature of humancentric LBS requires the public to assess the technology in terms of its socio-ethical implications so that it can benefit from its implementation and mitigate or avoid its detrimental effects. The qualitative content analysis performed revealed that there has been only limited discussion on the socio-ethical implications of location based services for humancentric tracking and monitoring. However, from this note we are able to draw an outline of the socio-ethical landscape of the possible implications of this technology, and point to the discernable weak spots if left unchecked.

-
- [1] B. Davis, Technoism: will the loss of freedom unleash the voice of dissent? International Symposium on Technology and Society: Crime Prevention, Security and Design. 26-28 September (2003) 19- 24.
- [2] K. Krippendorff, Content Analysis: An Introduction to its Methodology, Sage Publications, Beverly Hills, 1980.
- [3] Leximancer, Leximancer: From Words to Meaning, <http://www.leximancer.com/cms/> (2007).
- [4] A. Smith, Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping, Behavior Research Methods. 38 (2006) 262-279.
- [5] A. Smith, Use of automated content analysis techniques for event image assessment, Tourism Recreation Research. 30 (2005) 87-91.
- [6] G. Kaupins, R. Minch, Legal and ethical implications of employee location monitoring, Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 3-6 January (2005) 133a.
- [7] G.D. Smith, Private eyes are watching you: with the implementation of the E-911 mandate, who will watch every move you make? Federal Communications Law Journal. 58 (2006) 705.
- [8] A. Masters, K. Michael, Humancentric applications of RFID implants: the usability contexts of control, convenience and care, The Second IEEE International Workshop on Mobile Commerce and Services. 19 July (2005) 32-41.
- [9] Y. Xiao, X. Shen, B. Sun, L. Cai, Security and privacy in RFID and application in telemedicine, IEEE Communications Magazine. 44(4) (2006) 64-72.
- [10] A. Masters and K. Michael, Lend me your arms: the use and implications of humancentric RFID, Electronic Commerce Research and Applications. 6(1) (2007) 29-39.
- [11] C. Perakslis, R. Wolk, Social acceptance of RFID as a biometric security method, International Symposium on Technology and Society: Weapons and Wires. 8-10 June (2005) 79-87.
- [12] D.J. Glasser, K.W. Goodman, N.G. Einspruch, Chips, tags and scanners: ethical challenges for radio frequency identification, Ethics and Information Technology. 9(2) (2007) 101-109.
- [13] C. Soanes, A. Stevenson (Eds.), The Oxford Dictionary of English, Oxford University Press, Oxford, 2007.
- [14] R.N. Mayer. Technology, families, and privacy: can we know too much about our loved ones? Journal of Consumer Policy. 26, (2003) 419.
- [15] L. Perusco, K. Michael, M.G. Michael, Location-based services and the privacy-security dichotomy, The Third International Conference on Mobile Computing and Ubiquitous Networking. 11-13 October (2006) 91-98.
- [16] J. Weckert, Trust and monitoring in the workplace, IEEE International Symposium on Technology and Society. 9 August (2000) 245-250.
- [17] L. Perusco, K. Michael, Humancentric applications of precise location based services, IEEE International Conference on e-Business Engineering. 12-18 October (2005) 409-418.
- [18] G. Borriello, RFID: tagging the world, Communications of the ACM. 48(9) (2005) 34-37.
- [19] L. Perusco, K. Michael, Control, trust, privacy, and security: evaluating location-based services, IEEE Technology and Society Magazine. 26(1) (2007) 4-16.
- [20] O. Gunther, S. Spiekermann, RFID and the perception of control: the consumer's view, Communications of the ACM. 48(9) (2005) 73-76.
- [21] J.E. Dobson, P.F. Fisher, Geoslavery. IEEE Technology and Society Magazine. 22 (2003) 47-52.
- [22] E.M. Dowdell, You are here! - mapping the boundaries of the Fourth Amendment with GPS technology, Rutgers Computer and Technology Law Journal. 32(1) (2005) 109-139.

-
- [23] V. Lockton, R.S. Rosenberg, RFID: the next serious threat to privacy. *Ethics and Information Technology*, 7 (2005) 221-231.
- [24] S.L. Garfinkel, A. Juels, R. Pappu, RFID privacy: an overview of problems and proposed solutions, *IEEE Security and Privacy Magazine*, 3 (2005) 34-43.
- [25] I.A. Junglas, C. Spitzmuller, A research model for studying privacy concerns pertaining to location-based services, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. 3-6 January (2005) 180b.
- [26] A. Stone, The dark side of pervasive computing, *IEEE Pervasive Computing*. 2 (2003) 4-8.
- [27] J. Ellul, *The Technological Society*, Knopf, New York, 1964.
- [28] M.G. Michael, K. Michael, A note on überveillance, in: K. Michael, M.G. Michael (Eds.), *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society*, Wollongong, Australia, 2007, pp. 9-26.
- [29] R. Clarke, Information technology and dataveillance, *Communications of the ACM*. 31(5) 1988 498-512.
- [30] R.E. Smith, *Privacy journal*, <http://www.privacyjournal.net/> (2007).
- [31] R.E. Smith, Scary stuff, *Forbes.com*, http://www.forbes.com/opinions/2007/11/21/privacy-surveillance-technology-oped-cx_res_1126privacy.html (2007).
- [32] R.E. Smith, New ways your privacy is being invaded, *Yahoo!Canada Finance*, http://ca.pfinance.yahoo.com/ca_finance_general/435/new-ways-your-privacy-is-being-invaded (2007).
- [33] C. Offman, You are tagged, *The National Post*, <http://www.nationalpost.com/scripts/story.html?id=139966> (2007).
- [34] ABC. You're being watched right now: in an era of 'Internet everywhere' everyone is being tracked all the time, *ABC News*, <http://abcnews.go.com/Business/FunMoney/Story?id=3937203&page=2> (2007).
- [35] Aurora. 'Überveillance' replaces surveillance, *The Midnight Sun*, <http://www.themidnightsun.org/?p=1450> (2007).