2011

Editorial: The social and behavioural implications of location-based services

Katina Michael
University of Wollongong, katina@uow.edu.au

M G. Michael
University of Wollongong, mgm@uow.edu.au

Publication Details

Guest Editors Katina Michael & M.G. Michael (2011): The social and behavioural implications of location-based services, Journal of Location Based Services, 5:3-4, 121-137

Editorial: The social and behavioural implications of location-based services

Abstract
The social and behavioral implications of location-based services (LBS) are only now beginning to come to light in advanced markets where the services have been adopted by just a little over half the market (Microsoft 2011). Depending on one's definition of what constitutes location-based services, statistics on the level of adoption differ considerably. While it is helpful to provide as broad a list of applications as possible in what constitutes LBS (e.g. everything from in-vehicle navigation systems to downloading a map using a computer), it can also cloud the real picture forming behind this emerging technology. Emerging not in the sense that the technology is brand new, but emerging because the ensemble of technologies known as LBS are increasingly lending themselves to new levels of integration and convergence.

Keywords
services, location, implications, behavioural, social, editorial

Disciplines
Physical Sciences and Mathematics

Publication Details
Guest Editors Katina Michael & M.G. Michael (2011): The social and behavioural implications of location-based services, Journal of Location Based Services, 5:3-4, 121-137

Title: The Social and Behavioral Implications of Location-Based Services

Guest Editors: Katina Michael, M.G. Michael

Author Affiliation: School of Information Systems and Technology, University of Wollongong, Australia

** no abstract as it is the editorial*

Introduction

The social and behavioral implications of location-based services (LBS) are only now beginning to come to light in advanced markets where the services have been adopted by just a little over half the market (Microsoft 2011). Depending on one's definition of what constitutes location-based services, statistics on the level of adoption differ considerably. While it is helpful to provide as broad a list of applications as possible in what constitutes LBS (e.g. everything from in-vehicle navigation systems to downloading a map using a computer), it can also cloud the real picture forming behind this emerging technology. Emerging not in the sense that the technology is brand new, but emerging because the ensemble of technologies known as LBS are increasingly lending themselves to new levels of integration and convergence.

Location Based Tracking and Monitoring

This special issue is dedicated to location-based tracking and monitoring, and covers both the technical challenges and social implications of this topic. If we consider railway tracks as a metaphor for location-based tracking, then a track is denoted by an originating point, individual way points which connected make up a route, and a terminating point. The verb to *track* means to follow the trail of an object or subject, typically in order to find them or note their location at various points along a course. Tracking someone via location services usually happens at discrete intervals but sometimes requires a real-time continuous mode. Location-based tracking is said to be a subset process of location-based monitoring (M.G. Michael et. al., 2008).

In business terms, the act of monitoring in this context can be broadly defined as the collection and analysis of location information to provide people or systems in an organisation with the ability to evaluate progress towards expected outcomes. A typical reason for location-based monitoring would be to account for the use of resources against delivery results. For instance, has a truck loaded with fresh produce reached the customer destination at the expected day and time? In this manner location-based monitoring is also linked to traceability. Monitoring allows for performance statistics to be generated on the state of a given person or thing involved in an individual process. The verb to *monitor* means to observe and check the progress of something over time; maintain regular surveillance over; and to listen and report on. Location tracking is concerned with the raw historical location data dump, whereas location monitoring has more to do with knowledge such as exceptions, alerts, and warnings based on a set of rules, normally bound by space and time.

"Mobility is a basic and indispensable human activity that is essential for us to be able to lead independent lives on a daily basis" (Kayama, Yairi and Igi 2003). So it can be reasonably established that there may be a need for people and things to be tracked as they are intertwined within life-sustaining and life-enhancing processes. People visit fixed locations in the form of buildings, residential dwellings, and the natural environment. En route to their final destination, finished goods are located in a manufacturer, packaged, shipped via several modes of transport to a wholesaler, distributed to a retailer, and finally purchased by a consumer. All of these movements can be tracked in

real-time, near real-time or on an ad-hoc basis. Over time we have the ability to learn significant user locations and predict user movements (Ashbrook and Starner 2002; Iqbal and Lim 2010). People are creatures of habit, and products in business move around with a defined purpose.

The ability to interconnect subjects and objects is increasingly becoming the mantra of the Web of Things and People (WoTaP) (K. Michael et. al., 2010). Michael and Michael (2010) argue that such overarching location tracking and monitoring is leading toward a state of uberveillance. The ultimate trajectory of uberveillance is considered to be a lowest common denominator hybrid tracking chip, injected into the human body or animals (domestic, farming, even wild species) or everyday objects. For now we can point to the realization of this embedded surveillance technology through state-of-the-art ID systems and location services which demonstrate in part the future possibilities of full-fledged uberveillance. The social and behavioral implications of this kind of pervasive and ubiquitous monitoring are the focus of this special issue.

Identifying Social and Behavioral Implications of LBS

In identifying the social and behavioral implications of location-based services one can point to classifications in previous works. Perusco and Michael (2007) classify the social implications of LBS into four areas: control, trust, privacy and security. In investigating the ethical implications of LBS, K. Michael et al., (2006), also classify implications into four areas: privacy, accuracy, property and accessibility. To this list have also been added additional dimensions such as technology, risk, legal and regulatory concerns.

The behavioral implications of location-based services, especially with respect to location intelligence and profiling have been studied previously with one participant in K. Michael et. al., (2006) and with dozens of participants between two and six weeks in duration in Fusco et. al., (2011) and Gasson et. al., (2011). Qualitative analysis applied on mobile and GPS data logs identify major points of interest (POI) and can determine personal data such as: place of residence and place of work, social status, family life and routine. POIs drawn from this type of data can also reveal more sensitive information such as: religion, sexual life, health, and commission of an offence, among other things. In this special issue, Clarke and Wigan consider the deep privacy impact of tracking where one has been and warn of the dangers of making sweeping assumptions (whether accurate or not) based on location behaviors and the harms that can come to an individual or to a group as a result. Subsequently, in another paper in this issue, Abbas provides empirical results on the social implications of location-based services after using three types of GPS data loggers to gather location data. She provides a timely look at the attitudes of the Generation Y user group and comes out with some particularly pertinent results. The popular belief that Generation Ys do not mind sharing their location with others outside their family and close friends is challenged.

LBS as a Disruptive and Transformative Innovation

LBS is not only a disruptive but also a transformative innovation. LBS is changing the way we do things, and changing them radically in every market segment- consumer, business, government and emergency services. Take for instance, the amalgamation between location services and social networking applications, giving rise to location-based social networks (LBSN). Or for example, the application of location-based body wearable technologies for gamers or sufferers of mental illness (O'Loan and Sandy 2011). Or the integration of physiological condition monitors and GPS hardware which measure the performance of athletes and their overall game productivity levels on the field (Dorries 2006). Or child safety location services which enable parents with the ability to do remote look ups of the “exact” real-time position of their offspring (Chen 2010 ; Guardian 2011). Or LBS national emergency warning systems that can provide sticky shadows letting a user know that the zone

they are approaching has had a confirmed case of severe acute respiratory syndrome (SARS) during a pandemic alert (Lui 2003). Commercial location services are increasingly being offered by operators in local markets, and enterprise-wide location services are now available in global markets crossing jurisdictional boundaries enabling rich business processes for large multinationals. These services are taking advantage of GPS chipsets, accelerometers and sensors tucked away neatly in smart phones or vehicles or other form factors (e.g. video and audio recorders (Looxie 2011), shoes (GTX 2011), clothes and bags, wristwatches and geographic data loggers no bigger than a thumb drive (Trackstick Online 2011)). All of these technologies are set to revolutionize the health and well-being industry (Loh, Schietecat, Kwok et al. 2005) and in particular will change the way that vehicle insurance premiums are determined (Teensurance 2011).

The paper in this special issue by Ketabdar, Qureshi and Hui demonstrates how technologies embedded in smart phones can be used to monitor human activity for emergencies and the positive social implications in this type of setting that can be gained by being able to identify user's, their location and their inferred condition. These three variables can grant a massive deal of information about the state of an individual and whether they are in danger and in need of urgent assistance. Ketabdar et. al., describe a motion analysis system they have developed, *Activity Monitor*, which can denote when a person is walking, resting, or engaged in high activity. Each type of activity is detected just by a user carrying a smart phone. The team from Deutsche Telecom emphasize that the activity recognition data collected from Activity Monitor is best combined with geographical location data that can provide a rich source for extracting contextual information. Of the importance of geographic location data for effective performance of Activity Monitor, the authors stipulate it is essential: "[i]f the user being monitored faces a certain physical problem, shock or fall, having geometrical location of the accident sent along with the other information (all sent by the mobile device) can significantly enhance the recovery and assistance process."

The Risks Associated with Using LBS

To a degree near-perfect omnipresence is possible by tracking what a person is doing, how they are doing it, and when they are doing it. But even in beneficial uses of LBS, we need to be mindful that there can be negative consequences. The technology can fail, and it can fail cataclysmically. Linking mission critical medical systems or emergency warning and alert systems to LBS is a complex matter, especially given that the technology is not always available and not always accurate. In fact, few service providers could ever guarantee 100% locational reliability. Here we have a value proposition that needs to be offset by matters pertaining to trust in the service and trust in the service providers (Aloudat and Michael 2011), as well as providing safeguards against privacy risks such as unauthorized personal locational disclosure (Michael 2009). It is important, however, to point to the possibility that all this monitoring might also mean that we become acutely aware that we are being constantly watched and expected to act in particular ways in particular situations (Michael and Michael 2011). This could ultimately impact on our own ability to be creative, be different, be diverse, and be our own person. It is not only the loss of privacy that is increasingly at risk, but also the wonder of improvisation. We will be playing to a packed theatre instead of being comfortable in our own skins and identities.

But there is another service type that has emerged over the last decade that is impacting upon how we have come to use location-based services at a practical level. These are the services that are generally considered "free to use", despite the very real hidden intangible costs. These are the services that people opt into on the basis that they will make their life easier and afford them a greater amount of convenience and provide for them detailed location chronicles, and increased collaborative and networking stealth. These LBS applications do not carry a monthly licensing fee, nor do they

seemingly force consumers to disclose personally identifiable information. These are the services that let people “check in” to a location, allow families to visit new destinations with great ease, enjoyment and safety. They also provide people with the ability to show up-to-the-minute status updates about where they are and what they are doing on their favorite social networking site. They are very much an integral part of the wireless Internet. It seems today, no matter the online application, that every service provider wants to have an uberview of a user’s current location and it now goes beyond the idea of cookies. Despite the gains, there is something sinister about this suite of offerings, at least on deeper analysis. The problem with these kinds of intelligent systems, as Gretzel (2011) puts it so well, is that they “capture information about their environment and their users … [which] can be highly personal, including the physical location of a tourist” .

Overt and Covert Location-Based Surveillance

For the greater part this breed of LBS applications are overt in nature. The user has in theory consented to their usage, has read an online privacy policy, and has agreed to particular terms and conditions of usage on a given web site. But what of those covert applications acquiring one’s location surreptitiously (Dobson and Fisher 2003)? There are also a range of location-based surveillance applications which have a covert use providing people with the ability to ping a friend’s location remotely without their knowledge. Often these covert applications are dismissed as the exception to the norm but case law is revealing otherwise. Employers, for instance, are tracking the GPS coordinates of their employees through the smart phones they supply them with and the GPS data logger units on the vehicles they drive. There is some evidence to suggest that not all employers are informing their staff they are using this functionality. Employers are also cross-checking to see if employees have demanded remuneration for hours of work they have clearly not been engaged in given their physical location (Stern 2007). Employees are being penalized for losses in productivity and load if the truck they are driving does not make it to a certain customer location on time (Geller 2005) or the driver has been found to be driving recklessly (Starcomm 2010).

Customers too are increasingly under the microscope through the use of GPS, either knowingly or unknowingly. For instance, in a case in the United States, rental car clients were being charged for “excessive wear and tear” if they went beyond particular speed limits or for driving the vehicle beyond particular geographic limits (Ramasastry 2005). American Car Rental charged its clients $150 each time they drove over 79 miles per hour for more than two minutes at a time. American’s subsidiary Acme Rental had installed GPS devices in its cars to monitor the travel speeds of its customers. Using GPS on rental vehicles, especially in campervan hire is now standard practice in some markets. In a non-commercial capacity, husbands, wives and partners are tracking one another to ensure that they are not being cheated upon or to assert additional control over the other (GPS Spouse Tracking 2008). In a recent court case in the United States, a woman tracked her husband whom she suspected was cheating on her, with a GPS tracker device in the glove box of a vehicle they co-owned. The case went to court, and Mr Villanova sued for invasion of privacy but the judges ruled that what Mrs Villanova did with the GPS was not breaking the law. In a landmark case the three judges “decreed that the GPS was not an invasion of privacy because it only tracked Villanova in publicly viewable locations, not in some recondite cupboard or well” (Matyszczyk 2011). Parents too are supplying their children with smart phones with onboard applications that allow them to be tracked without their knowledge (China Everest 2011; KidTrack 2011), making sure they are keeping to the house rules that have been set (Abbas, Michael, Michael et al. 2011).

All of these applications signal a radical change in the fundamental dynamics in relationships, both in the private and corporate spheres and have the ability to severely impact on the traditional intuitive codes and message models of our day-to-day communication. We are not referring here to the

disclosure of personal information alone but to those undisclosed location disclosures between two or more people that have to do with trust. In essence LBS can be applied as an umbrella-like control mechanism to any mobile application area. Control, to ensure that workers are not conspiring against an organization after hours (Lee 2011); control over where a partner can and cannot visit; and control over a child's every move. Of course, "control" is not a bad thing under all circumstances, we must all abide by rules whether in our family group or in society at large, but the powerful will normally seek to exercise control over their subordinates and this will invariably mean the abuse of power. Control also underpins almost all commercial and government LBS applications even if they are primarily linked to convenience and care solutions (Masters and Michael 2007).

While organizations in particular attempt to become more efficient at what they do, reach economies of scale through technology, it cannot happen without the willingness of humans in a given business process. People are not programmed robots. LBS applications can point to optimal driving times given speed constraints for a given distance via a shortest path route, but the human factor needs to be considered and ample time given for drivers to reach a destination without feeling their every move is being scrutinized. The other issue is that the technological elite will always have the upper hand over those not yet versed in Network-speak. It means that an individual who uses their smart phone just to make phone calls could be oblivious to the fact that their mobile had been confiscated minutes earlier, either physically or using Bluetooth, and a small application enabling 24x7 remote monitoring downloaded. Notifications of latest downloads are good to alert users to what previous activity has occurred on their phone, so are email messages warning of the "location sharing" capability as being active, but even these will not work in the vast majority of cases either because people are not aware or just do not have the time to be examining changes to settings, recent downloads, and software updates. Perhaps the biggest risk to the future of LBS is locational data impairment- either through deliberate fabrication, computer virus, accidental deletion or inappropriate obfuscation.

Circumstantial Evidence Gathering and Location-Based Profiling

A new breed of systems have also burst onto the market such as radio-frequency identification (RFID) tags and transponders, automated number plate recognition systems (ANPR), assorted biometric recognition systems, and near-field communications (NFC)-based technologies to name a few. Location-based services are not just those that provide real-time and continuous tracking through mobile phones (Wigan and Clarke 2006). This is a widespread fallacy. The frequency of a time stamp does not determine validity, although at least three waypoints are required to create a track- an originating point, a midpoint, and a terminating point. When considering the admissibility of digital evidence in a court of law, a time stamp and location stamp determined by the physical address of an infrastructure asset such as an e-tollway gantry, may be of greater probative value than gathering a location breadcrumb where the accuracy and context is unknown (Bassiouni 2003). Location-based services are those systems that can also geographically locate a luggable or wearable or implantable device, on or in a person, animal or thing (e.g. a vehicle) to a physical address. Increasingly LBS technologies have been instituted using plain old closed circuit television (CCTV) capabilities that can recognize an individual to a location in a shopping centre or street lamp-post. Location-based profiling can be generated for several minutes, several hours, a day, a week, a month or a year(s) and dependent on the collection and storage of the information in a given system, data can reveal a variety of user patterns, trends and behaviors (Hildebrandt 2006). Beyond statistical data, location intelligence "reveals a great deal about one's preferences, friends, associations, and habits" (Otterberg 2005, 663).

Automatic Teller Machines (ATMs), Electronic Funds Transfer Point of Sale (EFTPOS) units and Government Interactive Web Kiosks, give us transaction histories and tell us with some confidence where a cardholder last withdrew monies or made a government service inquiry. A pattern may emerge

of a cardholder's weekly routine: fill the car with fuel at service station 'x', drop off the kids at school some distance away, then drive to work and back home, go shopping at the nearest mall for the weekly groceries, check-in to a government web kiosk to ensure family payments arrived, and enjoy some live entertainment at the theatre on the weekend, paying mainly with a credit card. In-vehicle RFID tags have also been used to prove the time, direction, and location in which a vehicle of a suspect was traveling shortly before the approximate time of a criminal or civil offence. The RFID exit and entry gantries on highways can tell us where a vehicle has been and has not been, at least with some level of certainty, and whether or not a driver has broken speed limits on the way through. For instance, court cases in the U.S. have already demonstrated the potential for toll-tracking information to be used to verify an individual's whereabouts and movements. The states of Delaware, Illinois, Indiana, Maryland, Massachusetts, New York and Virginia have all released E-ZPass toll records in response to court orders for civil matters, such as divorce. The states of Maine, New Hampshire, New Jersey and Pennsylvania only release electronic toll records for criminal cases (Newmarker 2007). Electronic passports at airports and RFID badges in organizations that are coupled with smartgates are also a rich source of information.

Assorted biometric recognition systems are now becoming very popular, especially in instituting government-to-citizen services. Scanning someone's hand or face or whole body can pinpoint that individual to a kiosk, a prison ward, a crowd, or a country. Mobile scanners that can scan a person's iris from about four feet away have also been developed (Charette 2011). The continual integration and recombination of these technologies is providing even more sophisticated tracking capabilities. Take for example, the ANPR system that will be tracking all Bay State drivers in Massachusetts (Riley 2011; O'Ryan and Chabot 2011) looking for those who are driving uninsured or unregistered vehicles. It may not be long before ANPR is integrated with facial recognition software to prove that it was a given person driving a particular vehicle at a certain point in time and place. The same goes with the endless possibilities of mobile point of view (POV) audio-video recorder footage whether body wearable or in-vehicle (RoadHawk 2011). Algorithms are increasingly being developed to attempt to identify people within a crowd, such as in a large stadium, protest march, or point of interest. Agre (2001) argues that "[f]ace recognition systems in public places… are a matter for serious concern." He noted the use of biometric capabilities during the 2001 Super Bowl, where spectators were unknowingly matched against a database of alleged criminals. These are real systems and they have real implications (Leman-Langlois 2003).

The Social Responsibility of Corporations Acquiring and Using Location Information

Despite the rhetoric of most companies that gather location-based data- that they are seldom interested in a single individual's personal information and all records are anonymous- it makes common sense that location-based advertising and marketing is best delivered in a personalised manner. Once companies have intimate knowledge about how we go about our day, which places we visit and how long we stay there, who else is with us at a given time in the day (i.e. "friends"), and what opinions we might hold about a given destination, then profiling can work to create responses that best exploit the user. Exploitation can occur in a variety of ways, for example: (i) by exploiting someone's impulse to spend on a given item(s) in a given store while they are out and about; (ii) by providing information to the user that may legitimize a particular behavior as a result of a weakness or passion (e.g. location-based gambling); and (iii) by harnessing the dynamics of groups knowing more about the background context of individual personalities based on location information. In essence we are referring here to the most sophisticated levels of information manipulation or even disinformation conveyed to users, inherently encouraging particular types of actions to be taken.

Web services in particular will underpin the execution of complex personalized processes. At the same time aggregated locational data plus other transaction data (e.g. from social networks) will be used to legitimately optimize services for a given context, but with the downside that they will also be used to sway consumer sentiment in this direction or that. Social media marketing analytics will play a particular role in gathering the opinions of networks and groups. Recording someone's location as they walk the streets, and noting their personalized sentiment data, will provide a geographical footprint overlaid with a running commentary that will be metaphorically akin to knowing the intricate and intimate details of a person's DNA structure. As Otterberg foresaw in 2005: "[t]he resultant lengthy, detailed record of one's location then provides a comprehensive picture of one's life. Location information reveals everything from daily habits like stopping at the same coffee shop on the way to work, to associations with other people, to visits to locales that reveal much more about a person's particular characteristics, affiliations or beliefs—such as a gay bar, a certain church, synagogue, or mosque; a strip club; or various political and civic organizations".

It is also true that our wireless-enabled netbooks and laptops that we lug around with us from one appointment to the next reveal a great deal about our movements. Wireless access points and signal strength algorithms can determine our location with accuracy but the reverse is also possible. Wardriving is a collection of information and resources pertaining to the activity of driving around in a car searching and pinpointing the location of a wifi network. The act of wardriving can be done using a vehicle, public transport, even on foot. Many wardrivers use GPS devices to measure the location of the network and log it on a website to form maps of the network neighborhood. In that manner wardriving allows people or organizations to match up the civic address, pinpoint longitude and latitude coordinates, even images like street views or council cadastre blocks with personal identifiable information of the householder. The value returned from wardriving is typically a network ID. The more network IDs one can collect, the better their geolocation system. With these geolocator systems you can find the position of a friend, provide navigation information, and geotag. Geotagging people to images and places, and using location-enabled video recorders is further changing the nature of LBS. It will not be long before we are locating people to the nearest powerpoint or light switch in the home, office or mall- to physical conduit touchpoints or other infrastructure elements in the creation of symbolic location coordinates in smart spaces (Stirbu 2009).

Large technology companies like Google, Apple and Microsoft have all come under fire in different jurisdictions for their collection and storage of various levels of location data captured using different methods. In the case of Google, data was said to have been collected accidentally while Google Street View cars took photographs of houses throughout the globe. According to McCullagh (2011), "[t]he cars were supposed to collect the locations of Wi-Fi access points. But Google also recorded the street addresses and unique identifiers of computers and other devices using those wireless networks and then made the data publicly available through Google.com [until recently]." Now that the company has pledged to no longer collect Wi-Fi data via its Street View vehicles, it is relying on user participation via Android handsets to get the information. "When phones running the Google OS detect any wireless network, they beam its MAC address, signal strength and GPS coordinates to Google servers, along with the unique ID of the handset" (Goodin 2011). It is wardriving by smart phone, and the problem for now is that there seems not to be any opt-out mechanism for users. Android handsets record about 50 base station tower entries and up to 200 wi-fi network IDs per day.

In the case of Apple, location data was being stored on the iphone and ipad and able to be downloaded onto a desktop computer. Despite that Apple has now lost a court case in South Korea over the location storage issue, their Q&A on the topic still states: "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so" (Apple 2011). Apple instead shifted the blame

to the industry at large stating: "[p]roviding mobile users with fast and accurate location information while preserving their security and privacy has raised some very complex technical issues which are hard to communicate in a soundbite. Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date." However the telecommunications regulator in South Korea did not agree with Apple Inc., and fined the company three million won (US$2,800) for allegedly collecting the location data of iPhone users in the country (Lee 2011). Given the measly amount, the fine is seen by observers as a warning for the tech giants to act in a socially responsible manner. Consumers are for the greater part oblivious to these forms of surveillance, whether accidental or deliberate. Even if "location enablement" is switched off by the user, there is still the likelihood that the service provider, or technology provider, is still watching which makes a mockery of the notion of a privacy policy. After a four month investigation by Korea's Communications Commission (KCC), it was declared that even if "iPhone users disabled location systems on their handsets, Apple collected users' whereabouts from June 22, 2010, through May 4, 2011" (Lee 2011). Like Google and Apple, Microsoft also announced that it collected the physical location information of customers who used its mobile operating system but that they had never stored user location histories directly onto the device (McCullagh 2011).

The Probative Value of Location Based Evidence in Convicting Criminals in Court

As much as a user's location information is noted as being personal and highly sensitive, it has been used by the courts to convict criminals. Consider for instance, two landmark U.S. court cases where GPS data led to murder convictions- in 1999 *State v. Jackson* and in 2003 *State v. Peterson*. In the Jackson case a judge executed a search warrant on Jackson's vehicles and residence for ten days, and then subsequently granted two more warrants which were extensions of time for the police to continue with covert surveillance (Blocker 2003). During the investigation, Jackson drove his truck back to the scene of the crime twice, where the body of his nine year old daughter was discovered by police in a shallow grave. When the Jackson case ended, there was some contention in the Washington Supreme Court on whether or not a warrant was required to place a GPS device on a person or vehicle (George 2003). In another case in New York in the same year, the judge ruled that police did not need a warrant to track Robert Moran on a public street, stating that the defendant: "… had no expectation of privacy in the whereabouts of his vehicle on a public roadway" (McCullagh 2005). Moran, a lawyer, was later charged with selling the methamphetamine drug.

In San Francisco, Scott Peterson had a GPS tracking device placed on his car for four months after being suspected of murdering his pregnant wife in 2002 (Dornin 2004). His suspicious behavior led to a legal trial involving much speculation over the use of the GPS antenna (even though police had a warrant), and the accuracy of the collected data. An expert witness was brought in by the prosecution, a staff scientist who made GPS components, who testified that to his knowledge there were at least three "glitches" during the time Peterson was being tracked. But the prosecution emphasized that the malfunctions only "amounted to about 11 minutes of inaccuracies out of hours of reliable tracking information" (Finz and Taylor 2004). Based on the evidence, the judge ruled that the technology was "generally accepted and fundamentally valid" (MSNBC.com 2004).

In the U.S. the fourth amendment protects against unreasonable search and seizure, but in 2007 the seventh circuit judges ruled that the placement of a GPS tracking device without the suspect's knowledge, did not qualify as a search of his car. This was the first time the seventh circuit weighed in on the issue, which other circuits had been split on. The court equated GPS tracking to police physically following a car, or monitoring safety cameras to follow a car, neither of which amounted to illegal search and seizure (GPSTrackSys 2007). This draws the question then, whether or not community members have the same right to track their neighbor's vehicles covertly. The paper in this

special issue by Thurman takes a historical look at the legal implications of using GPS in the United States as a surveillance device and discusses the warranted and warrantless search of a person's real-time location and location history. The focus of the paper is on how the federal circuit for the District of Columbia, ruled on the *United States v Maynard* case, introducing a new approach to the Fourth Amendment. Thurman draws from US jurisprudence, "exploring the privacy and regulatory issues surrounding the use of locational tracking technology by law enforcement personnel and suggests considerations for the definition of limits on the use of GPS surveillance, both with respect to warrants and statutory regulation of surveillance powers."

Towards Real-time Proactive Location-Based Forensic Profiling

Today there are GPS tracking solutions that send data in real-time wirelessly, as opposed to having to download the data manually and then retrace the routes of those whose vehicles are being monitored (OzSpy 2011). At any given point in time we can do a lookup on a given user to see where they are and infer by their location the activity they are engaged in. But what about the ability to monitor people in real-time or prior to committing an act just based on their location and the context around them? While Hildebrandt (2011) refers to the notion of proactive forensic profiling, the possibility to conduct near-real time proactive location-based forensic profiling cannot be discounted. Hildebrandt calls this the "dilemma of the criminalization of future behaviors." A strong symbiosis between government and business has emerged for the purposes of national security since September 11. The link between smart phones and social networks is undeniable. The power of location-based social networks (LBSN) is now beginning to distinctly emerge both in the rapid organization of protests and in the investigation of crimes and public unrest. The possibility that a smart phone can be located "near" a scene of a crime (SOC) or near multiple scenes of unrest is now well and truly feasible. The possibility that messages may be intercepted based on their location and accessed to a particular application (e.g. Twitter, Facebook) is also possible.

Research in Motion (RIM) has stated that it will cooperate with the Home Office and UK police forces looking into how it's popular and very secure Blackberry Messenger (BBM) service might have been used to organize riots in the north of London from the 6th of August 2011 after which followed the police shooting of London man, Mark Duggan. In a statement, RIM disclosed: "[a]s in all markets around the world where BlackBerry is available, we co-operate with local telecommunications operators, law enforcement and regulatory officials" (Espiner 2011). In response to the BlackBerry announcement, the BlackBerry Blog was hacked by a group that call themselves TeamPoison. The hackers wrote: "You Will _NOT_ assist the UK Police because if u do innocent members of the public who were at the wrong place at the wrong time and owned a blackberry will get charged for no reason at all …. if you do assist the police by giving them chat logs, gps locations, customer information & access to peoples BlackBerryMessengers you will regret it…" (LA Times 2011).

In the Vancouver riots a few months prior, instead of the police asking for assistance from the telecommunications companies, they asked bystanders who witnessed the events unfold to take audio-visual footage of the riots, and were allegedly inundated with submissions. According to Reuters (2011): "[a] note on the VPD website thanked citizens for the overwhelming response, and begged their patience while police sifted through the footage." Some believed that the social networks played a role in further inciting the violence, as users began to geo-tag and geo-record riot scenes and post them in near real-time on Twitter and YouTube. The problem with this kind of crowd-sourced surveillance is that it presents a problem for policing resources to have to plough through the magnitude of submitted data. The submissions may also misrepresent what actually happened because cross-sectional video evidence always falls short of capturing the bigger picture. Individuals may be implicated from the footage that were not the cause of the major damage but got caught up in the hysteria and posed for

photographs in front of burning vehicles instead. Despite these shortcomings, there is no doubt that location-based services will play a major role in locating individuals during times of public unrest. While uberveillance lends itself to misinformation, misinterpretation and information manipulation, Harfield (2010) argues "that degrees of criminal harm have also intensified" so the new means of meta-analysis through information technology are justified, if conducted within the means of the law.

Ways Forward

In the end identifying and predicting what the social and behavioral consequences to LBS are and might be into the future, may lead us to act in one of three ways. First, we can take the "do nothing" approach and take the risk as social media commentator Danah Boyd suggests. We stop being obsessed by the consequences and see how far the new technologies might take us and what we might become or transform into as a result (Boyd 2011). While humans might not always like change we are by nature in a continual state of flux. We might reach new potentials as a populace, become extremely efficient at doing business with each other, and make a positive impact on our natural environment by doing so. The downside to this approach is that it appears to be an all or nothing approach with no contingencies built in. That, if the risks do not pay off as we imagine that they might, that we end up being a society that distrusts, that we break down the social fabric that we call networked groups, and allow ourselves to be taken control over by the techno-political elite (Michael and Michael 2006). For as Jacques Ellul forewarned: "what is at issue here is evaluating the danger of what might happen to our humanity in the present half-century, and distinguishing between what we want to keep and what we are ready to lose, between what we can welcome as legitimate human development and what we should reject with our last ounce of strength as dehumanization" (Ellul 1989).

The second option is that we let case law determine for us what is legal or illegal based on existing laws, or new or amended laws we might introduce as a result of LBS challenges. We can take the stance that the courts are in the best position to judge on what we should and should not do with LBS technologies. If we break the law in a civil or criminal capacity, then there is a penalty and we have Acts on Workplace Surveillance, Telecommunications Interception and Access, Criminal Codes, Surveillance Devices, Data Protection and Privacy, Cybercrime, among others that can guide us on what to do. There is also the continual review of existing legislation by law reform commissions and the like. New legislation can also be introduced to curb against other dangers or harms that might eventuate as a result of LBS. Taking this option, means that we identify precedence as the best judge of all. There has been a gradual change regarding the limits of police powers and how and whom law enforcement agencies can track using a GPS and for how long (Craddock 2005) but these have more recently given way to the public space versus private space debate allowing for lawful warrantless covert tracking of entities. Additional papers at the heart of this matter that readers should study include those of Hildenbrandt (2008), Herbert (2006), Ganz (2005) and Otterberg (2005).

The third option is that we can introduce industry regulations that stipulate how LBS applications should be developed (e.g. using privacy by design and ensuring privacy impact assessments are done before LBS commercial applications are launched), and that technical expectations on accuracy, reliability and storage of location data are met. It may even become mandatory for every commercial LBS application to undergo some form of scrutiny that at least holds the service provider accountable for issues to do with liability, inaccurate location readings, poor service quality, unauthorized access of location data, and the like. It might also be stipulated that policies identified by the LBS service provider become easier to read in plain language, identifying the risks of sharing location, and personalised social contracts being entered into that specifically state a user's preference on whether or not their location information is to be accessed or utilized by anyone, including the service provider and its affiliates. While for the greater part these regulations are not enforceable, they at least hold the

industry at large to a code of conduct that if broken can have legal repercussions such as fines and other penalties. It is important that location records remain private, are not hacked into, remain in a secure database if needed, and are not retained for any longer than they need to be, working in concert with laws. Cuijpers and Pekárek study two core elements of European data protection legislation, namely the Data Protection Directive and the ePrivacy Directive, pertinent to personal data, location data and traffic data. They observe that the current directives are unclear with respect to the new non-traditional players entering the LBS value chain and offer two possible ways forward for the revision of the European legal framework on data protection.

It is also important that the right balance be found between the use of new laws, regulations and technological safeguards so as not to stifle the LBS industry at large. Although obvious, it is important to note that none of these options are mutually exclusive- there is no silver bullet solution here. The final solution may well be at times to introduce industry regulations or codes, at other times to do nothing, and in other cases to rely on legislative amendments despite the length of time it takes to develop these. The guest editors of this special issue believe that we must continue to discuss and to ponder on what the social and behavioral implications of LBS might be and to learn from adopters what they are today. In many ways it is these users who will shape the future of LBS, along with the innovators who will push every boundary possible in the creative thinking process of developing new applications for a variety of segments and markets.

The final paper in the special issue is written by Evans who challenges the whole issue of privacy as a major concern in the deployment of LBS providing a critique contra Michael and Michael and others in the domain. Going back to Heidegger he applies an ontotheological framework to a study on LBSN. The counter-argument is necessary. This is debating in earnest with practical outcomes. To examine the LBS dilemmas from all sides and from as many different angles as possible. This means embracing interdisciplinary, multidisciplinary and transdisciplinary studies. There can be no single answer provided from a single lens when there are so many different agents and influences at work. This has been one of the significant contributions to recent thought, especially in the realm of a balanced critique of technology, by the ‘re-discovery’ of the Frankfurt School and its essential observation that sciences are not value-free.

Finally, the authors would like to thank the individual contributors of this special issue for their papers, and the reviewers who with care offered their guidance on how to improve the manuscripts. This collection of papers stands to represent the advancement of location-based services and the need to understand the social and behavioral implications of LBS as we head toward an uberveillance society.

References

Abbas, R., K. Michael, et al. (2011). "Emerging Forms of Covert Surveillance Using GPS-Enabled Devices." Journal of Cases on Information Technology **13**(2): 19-33.

Agre, P. (2001). "Your Face is not a bar code: Arguments Against Automatic Face Recognition in Public Places." Retrieved 8 August 2009, from http://dlis.gseis.ucla.edu/people/pagre/bar-code.html.

Aloudat, A. and K. Michael (2011). "Towards the Regulation of Ubiquitous Mobile Government: A Case Study on Location-Based Emergency Services in Australia." Electronic Commerce Research **11**(1): 31-76.

Apple. (2011). "Apple Q&A on Location Data." Retrieved 10 August 2011, from http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html.

Ashbrook, D. and T. Starner (2002). Learning Significant Locations and Predicting User Movement with GPS. Proceedings of 6th IEEE International Symposium on Wearable Computers, Washington, DC, USA, IEEE Computer Society.

Bassiouni, M. C. (2003). Introduction to International Criminal Law.

Blocker, K. (12 September 2003). "Brad Jackson denied new trial: Supreme Court also said police can't install GPS devices without warrants " Spokesmanreview.com Retrieved 11 August 2011, from http://www.spokesmanreview.com/news-story.asp?date=091203&id=s1409175.

Boyd, D. (2011). "The Unintended Consequences of Obsessing Over Consequences (or why to support youth risk-taking)." Retrieved 31 July 2011, from http://www.zephoria.org/thoughts/archives/2011/07/29/consequences.html.

Charette, R. (2011). "Here's Looking at You, and You, and You ... ." Retrieved 2 August 2011, from http://spectrum.ieee.org/riskfactor/computing/it/heres-looking-at-you-and-you-and-you-.

Chen, A. (2010). "nu.m8 GPS Child Locator Watch Review." The Gadgeteer Retrieved 11 August 2011, from http://the-gadgeteer.com/2010/03/19/nu-m8-gps-locator-watch-for-kids-review/.

China Everest. (2011). "Child safety mobile phone: GPS tracking." Retrieved 9 August 2011, from http://www.cemobilephone.com/china-child_safety_mobile_phone_gps_tracking_mobile_phone_watch_mobile_phone_everest_gw2318-18002.html.

Craddock, T. (2005). "Casenote: The Limitations on Police Regarding GPS Tracking Devices: A Necessary Hindrance?" Computer Law Review & Technology Journal **9**: 506-7.

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

Dornin, R. (2004). "Judge Allows GPS Evidence in Peterson Case." from http://www.cnn.com/2004/LAW/02/17/peterson.trial/.

Dorries, B. (2006). "Cricket's appliance of science " The Courier-Mail Retrieved 8 August 2011, from http://www.foxsports.com.au/cricket/crickets-appliance-of-science/story-e6frf3g3-1111112359539.

Ellul, J. (1989). What I believe. Grand Rapids, Eerdmans.

Espiner, T. (2011). "RIM helps police inquiries into London riots." ZDNet Retrieved 10 August 2011, from http://www.zdnet.co.uk/news/security/2011/08/08/rim-helps-police-inquiries-into-london-riots-40093642/.

Finz, S. and M. Taylor. (2004). "Peterson Tracking Device Called Flawed- Defense Wants GPS Evidence Shut Out of Trial." San Francisco Chronicle Retrieved 10 August 2011, from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/02/12/BAG7P4V69B1.DTL.

Fusco, S. J., K. Michael, et al. (2011). Monitoring People using Location-Based Social Networking and its Negative Impact on Trust: An Exploratory Contextual Analysis of Five Types of "Friend" Relationships. International Symposium on Technology and Society, Chicago, Illinois: 1-8.

Ganz, J. S. (2005). "Comment: It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices." Journal of Criminal Law & Criminology **95**: 1360.

Gasson, M. N., E. Kosta, et al. (2011). "Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) **41**(2): 251-61.

Geller, A. (2005). "Bosses Use GPS to Keep Sharp Eye On Mobile Workers." Detroit News Retrieved 9 August 2011, from http://www.detnews.com/2005/technology/0501/01/technology-46929.htm.

George, K. (2003). "Court Will Decide If Police Need Warrant for GPS 'Tracking'" http://seattlepi.nwsource.com/local/121572_gps12.html, Seattle PI, 12 May, 2003."

Goodin, D. (2011). "Google location tracking can invade privacy, hackers say." The Register Retrieved 9 August 2011, from http://www.theregister.co.uk/2011/04/22/google_android_privacy_concerns/.
GPS Spouse Tracking. (2008). "Monitor Your Spouse's Activities with our GPS Tracking Devices." Retrieved 9 August 2011, from http://www.gpsspousetracking.com/index.htm.
GPSTrackSys. (2007). "7th Circuit U.S. Court of Appeals Okays Surreptitious GPS Tracking by Police." Retrieved 1 October 2007, from http://gpstrackingsystems.biz/7th-circuit-us-court-of-appeals-okays-surreptitious-gps-tracking-by-police/25/.
Gretzel, U. (2011). "Intelligent systems in tourism: A Social Science Perspective." Annals of Tourism Research **38**(3): 757-79
GTX. (2011). "GPS Shoes." Retrieved 8 August 2011, from http://www.gpsshoe.com/.
Guardian. (2011). "Guardian Angel Features and Pricing." Retrieved 8 August 2011, from http://www.guardiannow.com/prodlist.asp.
Harfield, C. (2010). E-policing and the Social Contract. The Social Implications of Covert Policing (The Social Implications of National Security Series). C. H. Simon Bronitt, Katina Michael. Wollongong, University of Wollongong. **IV:** 105-20.
Herbert, W. (2006). "No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery." I/S: A Journal of Law and Policy for the Information Society **2**(2): 409-73.
Hildebrandt, M. (2006). "Profiling: from data to knowledge. Challenges of a crucial technology." Datenschutz und Datensicherheit **30**(6): 548-52.
Hildebrandt, M. (2008). "Ambient Intelligence, Criminal Liability and Democracy." Criminal Law and Philosophy **2**(2): 163-80.
Hildebrandt, M. (2011). Proactive Forensic Profiling: Proactive Criminalization? The Boundaries of Criminal Law. R. A. Duff, L. L. Farmer, S. E. Marshall, M. M. Renzo and V. V. Tadros. London, OUP**:** in press.
Iqbal, M. U. and S. Lim (2010). "Privacy Implications of Automated GPS Tracking and Profiling." IEEE Technology and Society Magazine **29**(2): 39-46.
Kayama, K., I. E. Yairi, et al. (2003). Semi-Autonomous Outdoor Mobility Support System for Elderly and Disabled People. International Conference on Intelligent Robots and Systems: 2606.
KidTrack. (2011). "GPS Tracking for Safety and Covert Application." Retrieved 9 August 2011, from http://www.kidtrack.com.au/gps-tracking-store/child-trackers/.
LA Times. (2011). "BlackBerry blog hacked after RIM helps police in London riots." LA Times Retrieved 10 August 2011, from http://latimesblogs.latimes.com/technology/2011/08/blackberry-blog-hacked-after-rim-helps-london-police.html.
Lee, J.-A. (2011). "South Korea Fines Apple Over iPhone Location Data." Retrieved 10 August 2011, from http://online.wsj.com/article/SB10001424053111903454504576485621621796198.html.
Lee, K.-S. (2011). "Interrogating 'Digital Korea': Mobile Phone Tracking and the Spatial Expansion of Labour Control." Media International Australia: under review.
Leman-Langlois, S. (2003). "The Myopic Panopticon: The Social Consequences of Policing through the Lens." Policing and Society **13**(1): 51-4.
Loh, J., T. Schietecat, et al. (2005). "Technology Applied to Address Difficulties of Alzheimer Patients and Their Partners. Proceedings of the Conference on Dutch Directions in Human Computer Interaction.
Looxie. (2011). "Looxie: Device." Retrieved 8 August 2011, from http://looxcie.com/index.php/device.
Lui, J. (2003). "Cell phone firm offers SARS alerts." Retrieved 8 August 2011, from http://news.cnet.com/2100-1039-997457.html.

Masters, A. J. and K. Michael (2007). "Lend Me Your Arms." Electronic Commerce Research Applications **6**(1): 29-39.
Matyszczyk, C. (2011). "Court: It's OK to use GPS to track cheating spouse." CNET News Retrieved 9 August 2011, from http://news.cnet.com/8301-17852_3-20078146-71/court-its-ok-to-use-gps-to-track-cheating-spouse/.
McCullagh, D. (2005). "Snooping by Satellite." CNET News Retrieved 10 August 2011, from http://news.com.com/Snooping+by+satellite/2100-1028_3-5533560.html?tag=sas.email.
McCullagh, D. (2011). "Street View cars grabbed locations of phones, PCs." CNET Retrieved 31 July 2011, from http://news.cnet.com/8301-31921_3-20082777-281/street-view-cars-grabbed-locations-of-phones-pcs/.
McCullagh, D. (2011). "Microsoft collects locations of Windows phone users." CNET Retrieved 31 July 2011, from http://news.cnet.com/8301-31921_3-20057329-281.html#ixzz1TdiXL4fD.
Michael, B. D. R. a. K. (2009). "The privacy-value-control harmonization for RFID adoption in retail." IBM Journal of Research and Development **53**(2): 8:1-8:14.
Michael, K., A. McNamee, et al. (2006). Location-Based Intelligence- Modelling Behaviour in Humans Using GPS. International Symposium on Technology and Society, Flushing, New York, IEEE Computer Society: 1-8.
Michael, K., G. Roussos, et al. (2010). "Planetary-scale RFID Services in an Age of Uberveillance." Proceedings of the IEEE **98**(9): 1663-71.
Michael, M. G., S. F. Fusco, et al. (2008). "A Research Note on Ethics in the Emerging Age of Uberveillance." Computer Communications **31**(6): 1191-9.
Michael, M. G. and K. Michael (2006). "National Security: The Social Implications of the Politics of Transparency." Prometheus **24**(4): 359-64.
Michael, M. G. and K. Michael (2010). "Towards a State of Uberveillance." IEEE Technology and Society Magazine **29**(2): 9-16.
Michael, M. G. and K. Michael (2011). "The Fallout from Emerging Technologies: On Matters of Surveillance, Social Networks, and Suicide." IEEE Technology and Society Magazine **in press**: 1-5.
MSNBC.com. (2004). "Jurors: Peterson's Stoicism Was the Final Straw." Associated Press Retrieved 11 August 2011, from http://msnbc.msn.com/id/6711259/.
Newmarker, C. (2007). Toll records catch unfaithful spouses. USA Today.
O'Loan, J. and A. Sandy. (2011). "GPS units being used to track mentally ill but Bligh Government refuses to use them for sex offenders." The Courier-Mail Retrieved 8 August 2011, from http://www.couriermail.com.au/news/queensland/offender-watch-out-of-step-with-technology/story-e6freoof-1226062975676.
O'Ryan, J. and H. Chabot. (2011). "State tries to address scanner concerns." Boston Herald Retrieved 11 August 2011, from http://bostonherald.com/news/regional/view.bg?articleid=1353463.
Otterberg, A. A. (2005). "Note: GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment." Boston College Law Review **46**.
OzSpy. (2011). "Real Time GPS Vehicle and Personal Tracker with Audio." OzSpy Retrieved 11 August 2011, from http://www.ozspy.com.au/products/7-Listening-Devices/184-Real-Time-GPS-Vehicle-and-Personal-Tracker-with-Audio/.
Perusco, L. and K. Michael (2007). "Control, Trust, Privacy and Security: Evaluating Location-Based Services." IEEE Technology and Society Magazine **26**(1): 4-16.
Ramasastry, A. (2005). "Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving? FindLaw (23 August 2005) <http://writ.news.findlaw.com/ramasastry/20050823.html> at 1 October 2007. ."

Reuters. (2011). "Social media and the Vancouver riots." Reuters Retrieved 9 August 2011, from http://blogs.reuters.com/mediafile/2011/06/20/social-media-and-the-vancouver-riots/.

Riley, D. (2011). "License plate readers help police scan 30 plates a second." The MetroWest Daily News Retrieved 11 August 2011, from http://www.metrowestdailynews.com/archive/x1498054455/License-plate-readers-help-police-scan-30-plates-a-second#ixzz1Ucz0TcJB.

RoadHawk. (2011). "Digital Driver Protection System." Retrieved 9 August 2011, from http://www.roadhawk.co.uk/.

Starcomm. (2010). "What is the difference between tracking and monitoring?" Retrieved 9 August 2011, from http://www.starcomm.com.ph/faq.html#what-is-the-difference.

Stern, A. (2007). " Man Fired Thanks to GPS Tracking (31 August 2007) <http://www.centernetworks.com/man-fired-thanks-to-gps-tracking Center Networks> at 1 October 2007."

Stirbu, V. (2009). NavTag: An Inter-Working Framework Based on Tags for Symbolic Location Coordinates for Smart Spaces. Lecture Notes in Computer Science: Ubiquitous Intelligence and Computing, Springer Berlin / Heidelberg: 265-79.

Teensurance. (2011). "Real-time GPS-based Vehicle Tracking." Retrieved 8 August 2011, from https://www.teensurance.com/beacon.aspx.

Trackstick Online. (2011). "Trackstick Mini: The GPS Tracking System Providing Value and Performance." Retrieved 8 August 2011, from http://www.trackstickonline.com/products/.

Wigan, M. and R. Clarke (2006). Social impacts of Transport Surveillance. The Social Implications of Information Security Measures on Citizens and Business (The Social Implications of National Security). K. Michael and M. G. Michael. Wollongong, University of Wollongong**:** 27-44.