University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

1-1-2011

Emerging forms of covert surveillance using GPS-enabled devices

Roba Abbas
University of Wollongong, roba@uow.edu.au

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

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

Anas Aloudat
University of Wollongong

Follow this and additional works at: https://ro.uow.edu.au/infopapers

 Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Abbas, Roba; Michael, Katina; Michael, M G.; and Aloudat, Anas: Emerging forms of covert surveillance using GPS-enabled devices 2011, 19-33.
https://ro.uow.edu.au/infopapers/2533

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

Emerging forms of covert surveillance using GPS-enabled devices

Abstract

This paper presents the real possibility that commercial mobile tracking and monitoring solutions will become widely adopted for the practice of non-traditional covert surveillance within a community setting, resulting in community members engaging in the covert observation of family, friends, or acquaintances. This paper investigates five stakeholder relationships using scenarios to demonstrate the potential socio-ethical implications that tracking and monitoring people will have on society at large. The five stakeholder types explored in this paper include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Mobile technologies such as mobile camera phones, global positioning system data loggers, spatial street databases, radio-frequency identification and other pervasive computing can be used to gather real-time, detailed evidence for or against a given position in a given context. There are currently limited laws and ethical guidelines for members of the community to follow when it comes to what is or is not permitted when using unobtrusive technologies to capture multimedia, and other data (e.g. longitude and latitude waypoints) that can be electronically chronicled. The evident risks associated with such practices are presented and explored herein.

Keywords

surveillance, forms, covert, emerging, devices, enabled, gps

Disciplines

Physical Sciences and Mathematics

Publication Details

Abbas, R., Michael, K., Michael, M. G. & Aloudat, A. (2011). Emerging forms of covert surveillance using GPS-enabled devices. Journal of Cases on Information Technology, 13 (2), 19-33.

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/2533

Emerging Forms of Covert Surveillance Using GPS-Enabled Devices

Roba Abbas, Katina Michael, M.G. Michael, Anas Aloudat
School of Information Systems and Technology, University of Wollongong, Australia

EXECUTIVE SUMMARY

This paper presents the real possibility that commercial mobile tracking and monitoring solutions will become widely adopted for the practice of non-traditional covert surveillance within a community setting, resulting in community members engaging in the covert observation of family, friends, or acquaintances. This paper investigates five stakeholder relationships using scenarios to demonstrate the potential socio-ethical implications that tracking and monitoring people will have on society at large. The five stakeholder types explored in this paper include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Mobile technologies such as mobile camera phones, global positioning system data loggers, spatial street databases, radio-frequency identification and other pervasive computing can be used to gather real-time, detailed evidence for or against a given position in a given context. There are currently limited laws and ethical guidelines for members of the community to follow when it comes to what is or is not permitted when using unobtrusive technologies to capture multimedia, and other data (e.g. longitude and latitude waypoints) that can be electronically chronicled. The evident risks associated with such practices are presented and explored herein.

Keywords: covert surveillance, scenarios, GPS, location-based services, smart phones, socio-ethical implications, trust, behavioral tracking, breadcrumb, people, relationships

BACKGROUND

The availability, prevalence and proliferation of mobile tracking and monitoring solutions enable community members to independently gather location data for their own needs. In the market today are commercially available devices and technologies such as global positioning system (GPS) data loggers, spatial street databases, mobile camera phones, and radio frequency identification (RFID) tags, which facilitate the collection and capture of data related to the location of an individual. The information gathered from these devices can potentially be viewed in real-time, and may relate to habits, behaviors and/or trends. Furthermore, the devices support the compilation, display and manipulation of the location data, resulting in improved processing capabilities, and the application of the data and devices in novel situations, such as the use of covert surveillance from within a community setting. That is, technologies that were once considered to be used purely for the purposes of policing have now deviated from the policing realm, and are now increasingly available to community members at large. Effectively, this grants individuals complete power in conducting independent, covert surveillance activities within their social network. However, these practices lack the professionalism, checks and constraints

afforded in the more conventional forms of (community) policing, thereby introducing exaggerated socio-ethical consequences. This paper introduces and demonstrates the potential for covert surveillance in the community through a set of socio-ethical scenarios, which enable the ensuing implications of covert surveillance within the community to be investigated.

SETTING THE STAGE

This paper explores the potential for covert surveillance within the community by way of demonstrative scenarios, which are supplemented by supporting literature, in order to draw out the emergent socio-ethical dilemmas. Scenarios have confirmed their value in previous studies regarding location-based and mobile tracking technologies to allow for an evaluation of the future social impacts of emerging technologies (Perusco & Michael, 2007) and to establish the need for privacy controls for location technologies (Myles et. al., 2003), rendering them a fitting explanatory tool for the purposes of this paper.

The scenarios developed below are based primarily on a societal relationships taxonomy, which defines the main social interactions or relationships amongst community members. The societal relationships taxonomy is modeled on categories utilized in a published study titled "The Next Digital Divide: Online Social Network Privacy", which focused on the use of online social networks (ONS) by young Canadians, and by organizations for commercial purposes (Levin et al., 2008). Importantly, the study evaluates the user's perception of risk and privacy protection in using OSN, requesting that respondents indicate their concern about who is granted access to their online information. The response categories provided are: (i) friends, (ii) parents, (iii) other family member, (iv) employer, and (v) people you don't know (Levin et al., 2008).

These categories have been adapted to form the societal relationships taxonomy for this paper, as they offer a representation of the major social relationships that exist, and therefore offer guidance and a comprehensive approach to developing the socio-ethical scenarios relevant to covert and mobile tracking. However, while the aforementioned study is centered on perceptions of risk and additional concerns in an online setting, this research deals with each of the stakeholder categories in a physical setting and thus the categories have been modified to focus on the distinct physical interactions or relationships that may exist in a community social network. The five stakeholder types explored in this paper include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Each of these stakeholder types is represented by a demonstrative scenario, which is constructed and explained using existing studies and literature.

FIVE SCENARIOS: THE POTENTIAL MIS(USE) OF GPS-ENABLED SMART PHONES BY COMMUNITY MEMBERS

This section discusses the stakeholder scenarios which are hypothetical cases whereby GPS-enabled smart phones might be used (or misused) by community members on one another for the purposes of covert surveillance.

Partner-Partner Context: The Suspected Cheating Husband

Ted Johnson had arrived home late from work three days in a row, and had not been himself for some time. After repeated attempts to find out what was wrong, Ted's wife Jenny was fed up with his claims that he was overloaded at work. After all, this was the first time in 17 years that Ted had worked overtime. Having heard about a new GPS logging device that could be purchased

from Target at an affordable cost, Jenny placed the device in Ted's car, behind the tissue box next to the back window where he was unlikely to notice the thickset unit. What if Ted had been lying to her? Jenny could not wait to confront him with details of his whereabouts if he was to show up late for dinner again. She was convinced he had something to hide; now she would have the proof...

Parent-Child Context: Child Safety and Peace of Mind

The past week had been a trying one for the residents of a regional town in New South Wales, Australia. Word had spread of a near-kidnapping close to the public school. A white van was said to have been lingering around the grounds and had attempted to abduct several children before staff were formally on duty. Mr and Mrs Kumar were concerned about their eleven year old son's safety, as he had to walk home alone from school. The Kumars had recently emigrated and both had to work to make ends meet. Rachna felt guilty being a working mother and wanted to protect her son from all harm at all times. After speaking to some of her colleagues at work, Rachna believed that if she was able to monitor her son unawares until he had reached home, that she would have some peace of mind that he was okay and not have to rely solely on his promise that he would go directly home after school. In just a few Internet searches, Rachna had found her GPS child locator device and discussed the possibility with her husband. The Kumars agreed to subscribe to a monthly plan, sew the device into an inner lining of their son’s schoolbag, and access the secure website while at work. Simple! The investment in the GPS, they thought, would be worth the safety of their only child.

Employer-Employee Context: Workplace Monitoring and Surveillance

Called into his manager's office, Tom slowly closed the door behind him. It was unlike Ms Sanders to call one-on-one meetings with her staff, particularly members of the Delivery Team. This made Tom a little nervous. He had not been in a conflict with anyone and was generally happy with his occupation. "Tom it has come to my attention that you have been in breach of your contract. I regret to inform you that we will have to let you go." Ms Sanders handed Tom a wad of documentation that looked something like mobile phone records with street addresses. The cover letter read, “Dear Mr Clancy: After a 6 month investigation into the corporate use of your vehicle, we regret to inform you that your contract with ACME has been terminated. We provide evidence for your misconduct in the attached documentation. You will be escorted out of the premises by security without an opportunity to return to your desk…”

Friend-Friend Context: Prankster | Gotcha!

This year, university friends Anna and Chris had been competing heatedly with one another to find out who could play the best practical joke. Having received a 'cool' GPS monitoring device for a class assignment about new innovations in IT, Anna thought it would be great to track Chris and show him that she knew where he had been, just like Big Brother! Step one was to hide the device without Chris knowing. This was easier than Anna had anticipated given how close they were and the fact that they would often work out at the university gymnasium together. Recovering the device two days later, Anna could not wait to show Chris a wall-sized spatial map with breadcrumbs and little annotated notes she had made making fun of particular points of interest (POI). Looking at the first three hours worth of data, she just had to laugh. Chris was so

predictable! Looking on, Anna noticed Chris had not traveled to Sydney on Wednesday, as he had mentioned. Why did he tell her that he would be away all day?

Stranger-Stranger Context: Covert tracking

Having recovered from his car accident, Benji had spent the last few weeks afraid to leave his home and even get behind the wheel. While his accident was minor and the damage to his car not even worth an insurance claim, Benji was a little disconcerted about the small external GPS device his mechanic claimed to have found under the body of his car. He lived in a friendly neighborhood and knew almost everyone there, so who could have an interest in tracking his every move? He pondered on the possibilities and while he had nothing to hide he did not know what to make of it all and whether or not he should even contact the police. Over the years he had had a few conflicts, both personal and professional, but it was unlikely that they would have warranted this conclusion, he thought.

THE SOCIAL IMPLICATIONS OF COVERT SURVEILLANCE

Having presented the five scenarios above, this section interprets the scenarios and presents a discussion of the socio-ethical consequences of covert surveillance by members of the community. Each scenario is in fact a stand-alone case in which readers can enjoy considering hypothetical possibilities, outcomes and solutions. The authors discuss the social implications of each case were it to occur in real life and use existing literature to support their claims.

Trust Implications in the Partner-Partner Relationship

The rapid development of mobile monitoring and tracking technologies is enabling a shift in adoption into new market segments. Traditionally covert surveillance technologies have been used by security/ law enforcement personnel but increasingly they are now being used by general members of the public. While noting the positive use cases of such technologies for law enforcement in particular, a number of concerns must still be addressed. Advanced technologies today are available commercially over the counter, normally require little knowledge to assemble or even to operate. Covert surveillance devices can be used for the purposes of spousal tracking (Dobson, 2009). Spousal tracking can be considered a form of “geoslavery”. Dobson and Fisher (2003) define geoslavery as the ability to monitor and control the physical location of an entity, effectively empowering the 'master' who controls the other entity or entities (the 'slave').

When discussing the husband-wife scenario, a multitude of products, such as commercially available GPS tools and digital cameras/mobile phones (providing still and video footage) can be used to track the whereabouts of a partner, essentially diminishing the amount of control the victim or 'slave' possesses. To some degree this places the slave at the mercy of the controller and in a precariously powerless position. Furthermore, an individual can gather evidence for or against a particular position, as implied in the partner-partner scenario. Jenny seeks 'proof' for her husband’s unusual absence, and her suspicions can be confirmed or refuted based on the findings coming through multiple information streams generated via technologies.

An immediate danger that can be observed in the partner-partner scenario or broadly in the tracking of family members is the threat of technology misuse (i.e. abuse in this context), and the potential to encourage suspicion and importantly distrust (Barreras & Mathur, 2007). In an article that describes the uses and privacy concerns pertaining to wireless location-based services, M.G.

Michael is quoted as saying "[t]he very act of monitoring destroys trust, [and] implies that one cannot be trusted" (Ferenczi, 2009, p. 101). This trust implication is an underlying theme in the partner-partner scenario, as Jenny is convinced that her husband is deliberately concealing his whereabouts, jumping to the conclusion that he may be lying, and thereby questioning his trustworthiness.

Apart from the potential for misuse and the trust-related implications, privacy is an imminent concern when covert spousal tracking takes place. Individuals tend to lobby for increased privacy when institutional surveillance and monitoring activities take place, but are generally less wary of such activities being employed by families, notably within parent-child and spousal/partner-partner relationships (Mayer, 2003). Technologies such as internet-based tracking, GPS, miniature cameras and genetic tests are intended to be used to increase levels of safety for individuals within a family unit, however, Mayer (2003) believes that this can be damaging in terms of privacy and safety, and may also affect trust between family members.

In the case of the partner-partner scenario, the result of selective and continuous monitoring of partners must raise concern over potentially damaging outcomes. In selective situations, there is the danger of incriminating a partner based on an incomplete story/picture or incorrect details. Continuous monitoring activities which involve 24/7 observation and two-way communication (Dobson, 2009) run the risk of being interpreted as excessive surveillance eventuating to excessive levels of distrust. This is a harmful outcome. Moreover, data that has been collected using GPS-enabled devices is not always accurate and can be manipulated to provide information that is in conflict with reality (Iqbal & Lim, 2008). This is a particularly relevant consideration in the partner-partner and remaining stakeholder scenarios. This scenario encourages a number of questions: What are the relationship-related consequences in using covert surveillance techniques in a spousal situation? How will technological inaccuracies be factored into the decisions made based on the collected data? Can a partner take the law into their own hands? What actions are triggered by the assumptions made by the partner? How serious are the repercussions, for instance, physical violence, separation or even divorce?

Consent and Control Implications for the Parent-Child Relationship

The convenience associated with GPS monitoring and tracking technologies simplifies the ease with which such technologies can be used by family members, particularly in the parent-child scenario. That is, GPS technologies that come in the form of handheld, wearable and embeddable devices may be used to track the whereabouts of children such as the Wherifone wireless device (Michael et al., 2006) and the Verizon Wireless Chaperone (Ferenczi, 2009). These applications can be deployed in many different ways both overtly and covertly depending on the use of the subscriber who is usually the ‘controller’ and not the ‘slave’ as distinguished in the partner-partner scenario above. Generally, parent-child solutions are promoted as being technologies that increase safety levels. For example, Barreras and Mathur (2007) review family tracking software that is intended to provide knowledge of the location of family members, in order to maintain and provide protection. The solution is primarily attractive to parents who wish to monitor their child's movements, relying on continuous updates and the presentation of information on a secure website, as was the case in the above scenario. There is the perception that these solutions will ensure children are accountable for their behavior. Some parent-centric community groups view the technology as aiding and enhancing traditional parenting tasks and reinforcing ideals in children of what is right versus what is wrong.

The benefits of GPS technologies in the parent-child scenario are therefore specifically evident in two situations. The first situational context is that GPS technologies and monitoring applications can be used to protect young children who travel unescorted. The second situational context is that GPS technologies can monitor young adults (e.g. driving behavior) using commercial and portable systems that are fairly inexpensive to implement and are rather discrete in physical character (Mayer, 2003). This makes GPS and monitoring technologies ideal for covert uses. Commercially attainable GPS devices come in a number of forms, varying in size, capacity and complexity. These devices can be carried and worn in overt scenarios, and be placed amongst personal items within bags. Alternatively these devices can be obscured from view, within a vehicle or sewn into the inner lining of a very thick coat or bag, making the device virtually undetectable. If we deviate slightly from the scenario presented in the parent-child case and consider a situation where a parent just placed a device in full view in a pocket of the child's bag, the integrity of the solution is questioned, given that children can remove or ask a friend to carry the device. Still, even if the GPS device is sewn into the inner lining of the bag being completely unobtrusive, the risk of wrong GPS readings is ever-present- someone else could carry the bag of the child, the bag can be left behind after a child wanders off (e.g. a bus stop) and more. Such a scenario also assumes that a child has a bag with him/her all the time, which is not the case during recess or lunch in primary or infants school.

While such technologies have been used by law enforcement agencies for some time, it should be mentioned that the commercial alternatives do not require a high level of technical sophistication to implement. However, what are the resulting affects on trust, privacy and family relationships in general? A study on parental monitoring and trust maintains that a parent's trust in their child develops based on three types of knowledge: concerns/feelings which are linked to the beliefs or values a child possesses; information concerning past violations; and knowledge of a child's daily activities in varying situations which is linked to responsibility and judgment (Kerr et al., 1999). Importantly, the latter is weighted as an important form of knowledge, and information can be elicited in a number of ways.

The information can be provided freely by the child, the parent can prompt the child for knowledge, or alternatively parental control techniques can be adopted where specific rules are imposed on the child. With the introduction of commercially attainable GPS technologies, the presented parent-child scenario proposes that a fourth method can be utilized to obtain knowledge of a child; that is, the use of commercial technologies implemented covertly. However, a major concern that emerges from this form of knowledge elicitation is: what contribution/impediment will this make to (a) parental trust, and (b) the trust a child has in their parent?

Applying these claims to covert tracking in the parent-child scenario, one can immediately pinpoint concerns regarding the covert tracking of children, particularly in view of trust. For instance, why did Rachna feel the need to use a device covertly, rather than rely on her son's account? Could she have been more transparent regarding her safety concerns? What would ensue if the child was to discover he was being tracked? Furthermore, what impact would excessive tracking have on the development of the child? Is child tracking eroding the idea of private space, and thus prohibiting children from developing fundamental skills? Michael and Michael (2009, p. 86) build on this notion of private space, in an article that discusses the privacy implications of "überveillance". Fundamentally überveillance is "an exaggerated, and omnipresent 24/7 electronic surveillance". The authors highlight the importance of being granted a private 'location' or space in which to flourish, develop and discover one's identity free from continual monitoring. With regards to the parent-child scenario, it is apparent that tracking

technology may prohibit children from learning or developing 'street smartness' and other vital skills. Therefore, in an attempt to protect their child from 'society', parents can simultaneously be impeding their child's development, and the manner in which they view the role of trust (amongst other things) in relationships.

When considering the parental position, it is important to note that the perception of their child and the associated level of trust they have would also be affected/altered in the process of practicing independent policing-style surveillance activities. While from the parental perspective, the attainment of knowledge contributes to a trusting relationship, Kerr et al. (1999) found that the source of such knowledge is an essential factor. That is, the spontaneous disclosure of daily activities is favorable to other sources of knowledge gathering, and correlates to higher levels of trust on the part of parents. In gathering knowledge, family members often utilize monitoring and tracking technologies in the interest of the safety of their loved ones and with the best intentions, but this is generally conducted without consideration of the damaging nature of such activities, relinquishing trust and privacy in the process (Mayer, 2003). Similar articles review the use of child trackers to allow parents to identify the location of their child on a map or request the location of their child at any given time, also flagging the related privacy and trust issues (Schreiner, 2007).

In the context of covert surveillance within a community setting, a number of questions are pertinent. What consequences arise when a parent has knowledge of the daily activities of their child (for both parties)? How will GPS and other related techniques perform as valid knowledge gathering sources? Will the technologies contribute to or impede trust in parent-child relationships? Have the child's rights been considered? What will be the long term effects of parental monitoring and the covert policing of children? Does the use of parental monitoring solutions encourage a false sense of security for parents, particularly given the risk of a criminal 'breaking' into or compromising the system?

Implications for Employee Autonomy in the Workplace Relationship

Emerging technologies facilitate not only the collection of employee data but the storage and processing of such information, raising apprehension over information being used for purposes other than the intended use (Levin et al., 2006). A primary example is the use of unobtrusive GPS devices for covert surveillance applications. In this situation, an employer may utilize employee location details to incriminate individuals or to ‘police’ the activities of their subordinate in an unauthorized fashion. This was the case in Tom's situation in the employer-employee scenario. The implications of employee monitoring in general are discussed in numerous studies, a selection of which are presented here, providing insights into the associated risks.

Chen and Ross (2007) discuss the concept of electronic workplace monitoring, including the tracking of Internet usage and email communications. Specifically, their study focused on variations in individuals' personalities and demographic factors which affect the manner in which individuals respond to being monitored at work. The research discusses the use of electronic performance monitoring technologies, including GPS for vehicle location tracking, presenting both the positive and negative consequences that may result from such activities, while introducing a framework for evaluating individual differences in order to predict reactions to being monitored. In reviewing the literature, Chen and Ross (2007) identify gains such as reduced crime, enhanced customer relationships and productivity improvements. Similarly, the risks are articulated and include negative behavioral impacts, attitudinal effects and ethical concerns.

Other scholars elaborate on such perspectives, and offer additional examination of the risks associated with unwarranted levels of employee monitoring. Kaupins and Minch (2005) focus on the use of emerging technologies to monitor the location of individuals in a workplace setting, focusing on GPS solutions (outdoor, broader scale) through to sensor networks (indoors). The authors also point to the legal and ethical implications of having Internet/email communications and general work behaviors monitored by employees, citing security, productivity/performance enhancements, reputation and enhanced protection of third parties as being the encouraging facets of employee monitoring. Kaupins and Minch's (2005) inverse argument examines privacy, accuracy and inconsistency as being significant concerns of monitoring practices, with privacy also being cited by Townsend and Bennett (2003) as a chief concern, inevitably resulting in an undesirable work atmosphere between employer and employee. Weckert (2000) also reports on trust-related issues emerging from excessive monitoring of employees, contributing to deterioration in professional work relationships. Herbert (2010) offers a fresh perspective and important contribution with his balanced work on "Workplace Consequences of Electronic Exhibitionism and Voyeurism" where he discusses the legal implications of electronic voyeurism including employer surveillance of employee workplace computer use and employee off-duty blogs and social networking pages.

While the above discussion has focused on the implications of monitoring from an employee perspective, some studies examine employer attitudes regarding the workplace privacy and monitoring/surveillance debate. For instance, the study conducted by Levin et al. (2006) revealed that while employers admitted to using monitoring and surveillance techniques for benefits such as safety and security, fleet management, and employee training and development, they did not actively exploit the secondary uses of the monitoring technologies. With respect to the use of GPS technologies, the interviewed employers considered GPS technologies as a supply chain and fleet management solution first and foremost. Devices such as commercial mobility solutions (including GPS devices and in-car units), digital cameras and mobile phones, and electronic tags collect adequate information about an employee which can be used to promote efficient work practices and accountability, whilst providing employers with real-time access to information. However, this does not eliminate the fact that GPS technologies can be used for secondary purposes, and moreover in a covert manner. This is particularly true in cases where employers provide employees with a mobile phone for work purposes but use the technology surreptitiously because the functionality exists. In the United States persons who have had their employment contract terminated due to location data have had either an executive managerial level position or operational position.

The implications of employee monitoring have been briefly identified above. It is imperative then to consider the covert surveillance angle with respect to the workplace surveillance and monitoring context. Deceptive or concealed monitoring and tracking may result in trust being diminished in professional relationships, even in situations where high levels of trust are pre-existing. This is due to the fact that location information is often assured as accurate, despite the potential for inaccuracies to exist regarding the whereabouts of an employee. For instance, in deconstructing the employer-employee scenario, Ms Sanders does not question the source and validity of her information. She was also not forthcoming with respect to how she came to be in possession of details to prove Tom was in 'breach' of his contract. Rather, she opted to act on the situational information immediately, concluding that her employee was 'guilty' of requesting remuneration for work he could not have completed, according to the logged location data.

Concerns inevitably escalate when covert means of tracking are present, based on the premise that secret or deceptive monitoring will affect openness between employer-employee relationships. This notion is alluded to by Herbert (2006) in a paper which examines the legal issues associated with human tracking technologies such as GPS, RFID, cellular technology and biometric systems. The author claims that tracking technologies enhance the power and control given to employers, and therefore secrecy is required to avoid employee backlash with respect to the installation of monitoring systems. Herbert further asserts that such systems allow employers to monitor not only work-related activities, but also personal data and habits, which can be compromised and result in subordinates seeking legal protection, and in essence rebelling against their employers. Therefore, it appears that there is the need for a more transparent approach. For example, Kaupins and Minch (2005) suggest the introduction of policy manuals and employee handbooks when implementing employee monitoring in the workplace. Other regulatory and policy issues need to be explored, and a practical and actionable solution be proposed, one which protects the interest of both stakeholders in the employer-employee scenario. The primary question posed is: How do employers reconcile the opposing ideas of protecting personal privacy with encouraging productive and efficient behaviors/attitudes in the workplace?

Privacy Implications in the Friend-Friend Context

Prior to engaging in a discussion of risks, it is necessary to reaffirm that GPS technologies are considered to add validity in particular contexts and an additional dimension and layer of precision that has previously not been available. If used in an overt manner, GPS monitoring devices can offer convenience in planning social events, and may in reality provide built-in safety and privacy features from a technical standpoint. As such, several GPS-based solutions and location technology vendors promote the safety angle in friend-friend scenarios, maintaining that privacy and safety are in fact enhanced, in that friends have power over who can access their location and assist in emergency or undesirable situations respectively (Schreiner, 2007).

The friend-friend scenario depicted in this paper, however, provides an alternative viewpoint with less desirable connotations. This scenario questions the amount of control individuals possess over their location data, specifically, who holds access to their personal location information and what they do with it. A valuable comparison is to evaluate similar concerns within the online social networking space, where individuals are able to select their 'friends' and define the level of access granted to them on an individual basis. This form of control is diminished in the friend-friend scenario. Anna was able to independently track Chris' location, while Chris was seemingly unaware and did not have the power to restrict such activities, as two-way agreement was not reached.

Given the covert nature of such activities, concerns regarding control are significantly enhanced, as covert policing in the friend-friend scenario prohibits individuals from retaining the right to limit access to their details. The detrimental outcome of this situation is a loss of privacy.

In a related study on privacy and location-based services, Myles et al. (2003) explore the challenges associated with protecting personal information and privacy in using location-based technologies, through the development of a system which provides individuals with control over how they disseminate location information. The authors claim that individuals must possess such control and be notified of requests to access information in order to maintain privacy. In the presented scenario, control would be compromised, with the emergent risks extending beyond privacy to lack of trust, suspicion, obsessive behaviors and fundamental consequences to the very nature of the social fibers that bring individuals together to form a relationship.

This encourages an enquiry into the nature of friendships where covert surveillance practices are employed in the community setting, posing the following central questions: To what extent is the boundary between the physical world, in which traditional friendships are forged, affected by the electronic world of GPS data logs and potentially incorrect location information? Given that friendships are built on trust, is this not an erosion of this fundamental core value?

Personal Security Implications for the Stranger-Stranger Context

The idea of being tracked by a third party in a public space is not new; however, with technologies capable of determining location with pin-point precision, the potential for third party tracking is increased, and to some degree facilitated. In a study which distinguishes between location tracking and position aware services, Barkhuus and Dey (2003) explain that location tracking services result in added privacy concerns, when compared to their 'position aware' counterparts. That is, location tracking services require a third party to track the position of an individual, as opposed to position-aware services in which the device can determine its own location (Barkhuus & Dey, 2003). This finding was mentioned with reference to family and friends determining the physical position of an individual. Inevitably the concerns increase when the idea of a stranger is introduced into the scenario.

A recent study focusing on personal information in online social networks reported that individuals are generally unconcerned with friends accessing their profile. Yet these same individuals also expressed having anxiety over other people viewing and retrieving their personal information; the most disconcerting was that group of people that accessed the personal information of a respondent they were not acquainted with (Levin et al., 2008). When such a relationship is applied to the physical setting, and with the addition of mobile monitoring and tracking solutions, this interaction is represented by the stranger-stranger scenario. This has personal security implications.

The family, friend and employee-centric scenarios have expressed the ease with which commercial solutions, such as GPS data logging devices, can be installed and utilized. These factors are highly attractive in the stranger-stranger situation, providing a vehicle for individuals to ascertain details about persons they do not know or are unfamiliar with, in a similar manner to what Benji experienced in the scenario after his accident. Such situations are typically characterized by malicious intent and involve improper conduct, usually of a deceptive nature. For instance, parents may seek location information to maintain the safety of their dependents. Similarly, friends may request geographic details for convenience purposes or to organize gatherings within their social network. However, in the stranger-stranger scenario, such motivations are invalid, as the concept of 'stranger' itself suggests unfamiliarity, the unknown and the accessing of information without consent. This scenario demonstrates that the stranger-stranger interaction requires covert activity, deception and intrusion in its most fundamental form, due to the fact that individuals are unlikely to part with personal details, particularly location, to those they do not know. The aspect of 'intrusion' is further highlighted by the scenario where the outcome is that Benji possesses a feeling of fear and victimization. Additionally, the installation of the device itself suggests that the 'victim' remains unaware of the activities occurring which is another pivotal concern.

It is once again useful to look to social networking tools for insights into how emerging technologies are adopted by community members, as valid parallels can be drawn in the stranger-stranger scenario. This is applicable given the scenarios discussed throughout this paper are based

on social interactions which are present and have become more clearly defined on social networking sites.

In a study which focuses on the features, history and literature regarding social networking sites, Boyd and Ellison (2008) identify the term "networking" to refer to the initiation of interactions between strangers; however, they go on to state that this is not the primary aim of such technologies. That is, social networking technologies are intended to support existing social networks, while encouraging and facilitating the ability for strangers to form connections based on some common interest. Importantly, the authors examine visibility and the public display of information as central themes within social networking technologies. In theory, these technologies provide users with the ability to grant and/or restrict access to their profile.

When such concerns are applied to GPS and location monitoring software, the nature of the terms are altered. That is, visibility and the display of information are now controlled by the individual who installs and possesses the device and related software, rather than the individual about whom the data is collected. Furthermore, the primary intention of monitoring and tracking solutions are to determine location, as opposed to forming networks and relationships, although solutions exist that provide both functions.

Consequently, the risks in the stranger-stranger situation are amplified, as they imply sinister connotations such as stalking, sabotage, fraud, crime, and surveillance. These evident risks cannot readily be justified or masked in any way. Strangers are therefore empowered to perform covert policing techniques within the community setting, with the capability and tools to control or influence the behavior of others. Such risks urge that safeguards be introduced to protect individuals from assuming the role of the victim in such a scenario. Further research is required to determine the intricacies of this stakeholder type, and to propose an enforceable strategy or legal framework that minimizes the risks, and inhibits strangers from utilizing mobile tracking and monitoring solutions for ill purposes. However, this remains a challenging area due to the difficulty in identifying offenders, and implementing pragmatic strategies that can be imposed on them.

CHALLENGES AND CONCLUSION

In drawing out the major themes from the scenarios and the related literature, it is valuable to consider the methodological process underlying the concept of covert surveillance, vis-à-vis a type of covert policing but within a community setting. Thus it is no longer law enforcement agencies that are empowered with technology, but all consumers who can afford the systems and technologies that can be used to observe and to watch "without ceasing". Figure 1 provides a summary of this conceptual process. The diagrammatic representation allows the following findings to be extracted. First, the conceptualization of the process while applied to covert surveillance/policing in this instance, is also applicable to other areas. Second, in discussing the implications associated with emerging technologies, researchers and other individuals must consider the fundamental technical context, the social/environmental context in which the technologies are situated, in addition to the socio-ethical scenarios that will inevitably emerge. These scenarios can be sourced from real life events early on in the proliferation of the new technology, some of which find themselves being documented in the courtroom. Third, all the implications recognized must take into account the positive applications of devices, in conjunction with the less desirable effects, to ensure a balanced evaluation of the emerging technology in a given context. Fourth, future studies must consider the nature of the linkages between each of the identified elements and address the policy, regulatory and legal concerns.

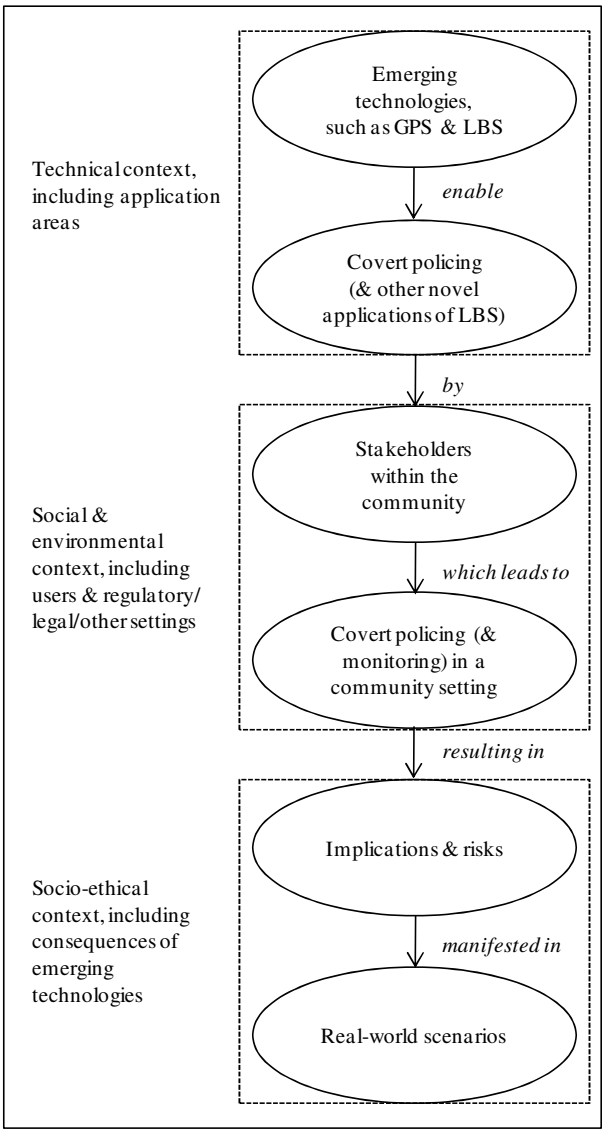

Figure 1. Conceptualizing the notion of covert policing within a community setting

Assessing the technical, social/environment and socio-ethical aspects allows us to draw a number of preliminary conclusions and themes from this study. First, GPS technologies contain vulnerabilities and are not error free. All systems can fail, and all systems are vulnerable. Thus in all the case scenarios, the 'victim' may be incriminated or judged based on incorrect information and evidence. Incorrect data can yield inaccurate or false behavioral patterns. That is, a digital location chronicle of an individual may not necessarily match the physical reality, and thus assumptions cannot be made without accurate contextual information and discussions as supportive evidence. Technological concerns aside, in applying solutions that were originally intended for law enforcement and covert policing purposes to the community setting, risks relating to relationships and interactions between stakeholders surface. That is, the notion of covert activities almost always implies some form of deception and hidden agenda, which contributes negatively to social relationships within a community environment. In the case of strangers, the issue is magnified and the psychological and legal ramifications are of primary

importance. Oppositely, when individuals are acquainted, the issues are intricately linked to changing the nature of personal relationships, concurrent with previously discussed factors such as privacy, trust and control. All scenarios point strongly to the need for some form of protection, and the introduction of safeguards that would minimize the adverse consequences, which may come in the form of legal (regulation), ethical (safeguards and/or privacy policies), or technological (default features such as warning systems) mechanisms, in order to protect the interests of community members.

REFERENCES

Barkuus, L., & Dey, A. (2003). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns, Proceedings of the 9th IFIP TC13 International Conference on Human-Computer interaction (INTERACT 2003), September 1-5 (pp. 709-712). Zurich, Switzerland: ACM Press.

Barreras, A., & Mathur, A. (2007). Wireless Location Tracking. In K.R. Larson & Z.A. Voronovich (Eds.), Convenient or Invasive- The Information Age (1st ed., pp. 176-186). Boulder, Colorado: Ethica Publishing.

Boyd, D.M., & Ellison, N.B. (2008). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication International Communication Association, 13(1), 210–230.

Chen, J.V., & Ross, W.H. (2007). Individual Differences and Electronic Monitoring at Work. Information, Communication & Society, 10(4), 488-505.

Dobson, J.E. (2009). Big Brother has evolved. Nature, 458(7241: Apr 23), 968.

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

Ferenczi, P.M. (2009). You are here. Laptop Magazine, February 2009, 98-102.

Herbert, W.A. (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, 2(2), 409-473.

Herbert, W.A. (2010). Workplace Consequences of Electronic Exhibitionism and Voyeurism. In K. Michael (Ed.), Paper presented at the IEEE Symposium on Technology and Society (ISTAS2010), June 7-9 (pp. 300-308). Wollongong, New South Wales, Australia: The Society on Social Implications of Technology, IEEE.

Iqbal, M.U., & Lim, S. (2003). Legal and Ethical Implications of GPS Vulnerabilities. Journal of International Commercial Law and Technology, 3(3), 178-187.

Kaupins, G., & Minch, R. (2005). Legal and Ethical Implications of Employee Location Monitoring, Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05), January 3-6 (pp. 1-10). Big Island, Hawaii: University of Hawaii.

Kerr, M., Stattin, H., & Trost, K. (1999). To Know You Is To Trust You: Parents' Trust Is Rooted in Child Disclosure of Information. Journal of Adolescence, 22(6), 737-752.

Levin, A., Foster, M., Nicholson, M.J., & Hernandez, T. (2006). Under the Radar? The Employer Perspective on Workplace Privacy. Ryerson University, June 2006. Retrieved March, 2009, from http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf

Levin, A., Foster, M., West, B., Nicholson, M.J., Hernandez, T., & Cukier, W. (2008). The Next Digital Divide: Online Social Network Privacy. Ryerson University, Ted Rogers School of Management, Privacy and Cyber Crime Institute, March 2008. Retrieved March, 2009, from http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf

Mayer, R.N. (2003). Technology, Families, and Privacy: Can We Know Too Much About Our Loved Ones? Journal of Consumer Policy, 26(4), 419-439.

Michael, K., Mcnamee, A., & Michael, M.G. (2006). The Emerging Ethics of Humancentric GPS Tracking and Monitoring, Proceedings of the International Conference on Mobile Business (ICMB2006), July 25-27 (pp. 34-42). Copenhagen, Denmark: IEEE Computer Society.

Michael, M.G., & Michael, K. (2009). Uberveillance: Microchipping People and the Assault on Privacy. Quadrant, LIII(3), 85-89.

Myles, G., Friday, A., & Davies, N. (2003). Preserving Privacy in Environments with Location-Based Applications. Pervasive computing, 2(1), 56-64.

Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: evaluating location-based services, IEEE Technology and Society Magazine, 26(1), 4-16.

Schreiner, K. (2007). Where We At? Mobile Phones Bring GPS to the Masses. IEEE Computer Graphics and Applications, 27(3), 6-11.

Townsend, A.M., & Bennett, J.T. (2003). Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy. Journal of Labor Research, 24(2), 195-205.

Weckert, J. (2000). Trust and Monitoring in the Workplace, Proceedings of the IEEE International Symposium on Technology and Society, University as a Bridge from Technology to Society, September 6-8 (pp. 245-250). Rome, Italy: The Society on Social Implications of Technology, IEEE.