Demonstrating the Potential for Covert Policing in the Community: Five Stakeholder Scenarios

Roba Abbas, Katina Michael and MG Michael
University of Wollongong

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 policing within a community setting, resulting in community members engaging in covert policing 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. However, 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 that can be electronically chronicled. The evident risks associated with such practices are explored.

Keywords: community policing, covert policing, scenarios, GPS, LBS, socio-ethical
1 Introduction

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 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, behaviours and 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 covert policing within a community setting. That is, technologies that were once considered components of professional policing and law enforcement strategies have deviated from the policing realm, and are now available to community members. Effectively, this grants individuals complete power in conducting independent, covert policing 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 socio-ethical consequences. This paper introduces and demonstrates the potential for covert policing in the community through a set of socio-ethical scenarios, which enable the ensuing implications of covert policing within the community to be investigated.

2 Method

This paper explores the potential for covert policing within the community by way of concise but demonstrative scenarios, which are supplemented by related 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 and Michael, 2006) 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 modelled on categories utilised in a recent study and report titled “The Next Digital Divide: Online Social Network Privacy”, which focuses on the use of online social networks (ONS) by young Canadians, and by organisations 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. However, while the aforementioned study is centred 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. Figure 1 identifies the systematic process adopted throughout this paper, displaying the relationship between the societal relationships taxonomy, literature and scenarios.

**Figure 1: Process and method used throughout this paper**

3 Scenarios

This section discusses the stakeholder scenarios, initially offering the concise scenario followed by a discussion of the socio-ethical consequences of covert policing in the community.

3.1 Husband-wife (partner-partner)

Scenario: Ted Johnson had arrived home late from work five days in a row, and had not been himself for some time. After repeated attempts to find out what was wrong his wife, Jenny, was fed up with Ted’s 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 was available for some three hundred dollars, Jenny placed the device in Ted’s car, behind the tissue box next to the back window where he was unlikely to notice the somewhat hefty unit. What if Ted had been lying to her? Jenny could not wait to confront
him with details of his location if this was to happen again. She was convinced he had something to hide; now she would have proof...

Developments in mobile monitoring and tracking technologies are enabling a shift from use by law enforcement/policing agencies to general members of the public. While noting the positive applications of such technologies for law enforcement and other situations, a number of concerns must be addressed. That is, technologies are now available commercially, require little knowledge of the technical aspects to operate, and can be used for purposes such as spousal tracking (Dobson, 2009). Spousal tracking can be considered a form of ‘Geoslavery’, which Dobson and Fisher (2003) describe 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. Furthermore, an individual can gather evidence for or against a particular case, as implied in the provided scenario through the concept of ‘proof’, and can confirm the findings through multiple means/technologies. An immediate danger that can be observed in this scenario or broadly in the tracking of family members is the threat of technology abuse, 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, it is argued that “The very act of monitoring destroys trust, implies that one cannot be trusted” (Michael in Ferenczi, 2009: 101). This notion is an underlying theme within the scenario, as Jenny is convinced that her husband is concealing his whereabouts, jumping to the conclusion that he may be lying, and thereby questioning Ted’s trustworthiness.

Apart from the potential for misuse and the trust-related implications, privacy is an imminent concern when spousal tracking takes place. Individuals tend to lobby for increased privacy where institutional surveillance and monitoring activities take place, but are less wary of such activities being employed by families, notably within parent-child and spousal/husband-wife relationships (Mayer, 2003). Technologies such as internet 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, safety, and may also affect trust between family members.

In the husband-wife scenario, one must raise concern over the potentially
damaging results of selective and continuous monitoring of partners. In selective situations, there is the danger of incriminating a spouse based on an incomplete picture or details. Continuous monitoring activities, which involve 24/7 monitoring and two-way communication (Dobson, 2009), run the risk of high degrees of surveillance and excessive levels of distrust, which is an unhealthy outcome. Moreover, data that has been collected using GPS-enabled devices is not always accurate and can be manipulated to provide information that conflicts with reality (Iqbal & Lim, 2008), a highly relevant consideration in the husband-wife and remaining stakeholder scenarios. This scenario encourages a number of questions: In using covert policing in a spousal situation, what are the relationship-related consequences? How will technological inaccuracies be factored into the decisions made based on the collected data? Will 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 or divorce?

3.2 Parent-child

Scenario: 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, and the Kumar family were concerned about their eleven year old son’s safety, as he had to walk home alone from school, given the current situation at home and the need for mum, Rachna, to be at work. Rachna felt that if only she was able to monitor her son unawares until he had reached home, she would have peace of mind that he was ok and not have to rely solely on his promise that he would go home directly after school. A few Internet searches later, she had found the answer. All Rachna had to do was subscribe monthly, place the GPS-enabled device in her son’s backpack, and access the secure website while at work. Simple! The investment would be worth the safety of her child...

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 come in the form of handheld, wearable and embedded 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), and can be deployed in many different ways, both overtly and covertly. 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 the solutions will ensure children are accountable for their behaviour, and some view the technology as aiding and enhancing traditional parenting tasks.

The benefits of GPS technologies in the parent-child scenario are therefore specifically evident in two situations, which include the protection of young children who travel unescorted, and also the monitoring of young adults using commercial and portable systems that are fairly inexpensive to implement and are rather discrete in physical characteristics (Mayer, 2003). This makes GPS and monitoring technologies ideal for covert uses, as 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 or obscured from view within a vehicle, making the device virtually undetectable. However, in the parent-child situation, the integrity of the solutions is questioned, given that children can remove or ask a friend to carry the device.

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 judgement (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 provided scenario proposes that a fourth method can be utilised 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) build on this notion of private space, in an article that discusses the privacy implications of ‘Überveillance’, which is considered, at the fundamental level, “an exaggerated, and omnipresent 24/7 electronic surveillance” (p. 86). 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 the child’s development, and the manner in which they view the role of trust (amongst other things) in relationships.

When considering the parent’s position, it is important to note that their perception of their child and the associated level of trust they have would also be affected/alter in the process of practicing independent policing activities. While from the parent’s perspective, the attainment of knowledge contributes to a trusting relationship, Kerr et al. (1999) found that the source of such knowledge in an essential factor. That is, the spontaneous disclosure of daily activities is favourable to other sources of knowledge gathering, and correlates to higher levels of trust on the part of the parents. In gathering knowledge, family members often utilise 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 policing 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 forms of technologies perform as a valid knowledge gathering source? 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 affects 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 tracking system?

3.3 Employer-employee

Scenario: 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...”

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 (Levin et al., 2006). A primary example is the use of unobtrusive GPS devices for covert policing applications. In this situation, an employer may utilise employee location details to incriminate individuals or to ‘police’ the activities of their subordinate in an unauthorised fashion, which was the case in Tom’s situation above. The implications of employee monitoring in general are discussed in numerous studies, a selection of which are offered below, providing insight into the related risks.

Chen and Ross (2007) discuss the concept of electronic workplace monitoring, including the tracking of Internet usage and email communications. Specifically, their study focuses 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 behavioural 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 (indoor). The
authors also point to the legal and ethical implications of having Internet/email communications and general work behaviours 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.

While the above discussion has focussed on the implications of monitoring from an employee perspective, some studies examine employer attitudes regarding the workplace privacy and monitoring/surveillance debate. For instance, Levin et al’s (2006) study 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 the GPS technologies can be used for secondary purposes, and moreover in a covert manner, particularly in cases where employers obtain a work phone without realising they can be tracked.

The implications of employee monitoring have been briefly identified; it is therefore imperative at this point to consider the covert angle with respect to the supplied scenario. Deceptive or concealed monitoring and tracking may result in trust being diminished in professional relationships, even in situations where high levels of trust exist. 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 did not question the source and validity of her information, in that she was not open with respect to how she came in possession of details to prove Tom was in ‘breach’ of his contract. Rather, she opted to ‘police’ the situation immediately, concluding that her employee was
guilty’ of requesting remuneration for work he could not have completed, according to the location data.

Concerns inevitably escalate when covert means of tracking are present, based on the premise that secret or deceptive monitoring will affect open transparent relationships, affecting employer-employee relationships. This notion is alluded to by Herbert (2006) in 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 behaviours/attitudes in the workplace?

3.4 Friend-friend

Scenario: 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 knows where he has been, just like Big Brother! Step one was to conceal the device without Chris knowing. This was easier than Anna had anticipated given how close they were. Recovering the device two days later, Anna could not wait to show Chris. 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 travelled to Sydney on Wednesday, as he had mentioned. Why did he tell her that he would be away all day?

The previous scenarios have alluded that emerging technologies are moving beyond government-related (and policing) applications, and are being applied in more family, friend and employee-centric applications (Barreras & Mathur, 2007).
The friend-friend scenario will further build on the identified risks and implications. Prior to engaging in a discussion of risks, it is necessary to point out the alternative and positive argument that such technologies may have. 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, 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 location information. 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; for instance, Anna was able to independently track Chris’ location, while Chris was seemingly unaware and did not have the power to restrict such activities, as it was not a two-way agreement.

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 behaviours and fundamental consequences to the very nature of social relationships between individuals.

This encourages an enquiry into the nature of friendships where covert policing 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?

3.5 Stranger-stranger

Scenario: Having recovered from his car accident, Benji had spent the last month afraid to leave his home. While his accident was minor and the damage to his car small, Benji was a little disconcerted about the small GPS tracker his mechanic found hidden under the body of his car. He lived in a friendly neighbourhood and knew almost everyone there, so who could have an interest in tracking his every move?

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.

A recent study focusing on personal information in online social networks reported that individuals are generally unconcerned with friends accessing their profile, but expressed anxiety over other people viewing and retrieving personal information, the most concerning being those that the respondent is 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.

The former scenarios have expressed the ease with which commercial solutions, such as GPS data logging devices, can be installed and utilised. 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. Such situations are typically characterised 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 organise 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 basic form, due to the fact that individuals are unlikely to part with personal details, particularly location, to those they do not know. The ‘intrusion’ aspect or theme is further highlighted by the scenario, the outcome of such intrusion being fear and victimisation. Additionally, the installation of the device itself suggests that the ‘victim’ remains unaware of the activities occurring, 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 notions 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 behaviour of others. Such risks urge that safeguards be introduced to protect individuals from assuming the role of the victim is 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 minimises the
mentioned risks, and inhibits strangers from utilising 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.

4 Discussion and Conclusion

In drawing out the major themes from the scenarios and the related literature, it is valuable to consider the thought process underlying the concept of covert policing within a community setting. Figure 2 provides a summary of this process. The diagrammatic representation allows the following findings to be extracted: (i) the conceptualisation of the process, while applied to covert policing in this instance, is also applicable to other areas; (ii) 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; (iii) the implications recognised must take into account the positive applications, in conjunction to the less desirable effects, to ensure a balanced evaluation of the emerging technology; and finally (iv) further studies must consider the nature of the linkages between each of the identified elements and address the policy, regulatory and legal concerns.

Assessing the technical, social/environment and socio-ethical aspects allows us to draw a number of preliminary conclusions and themes from this present study. Firstly, GPS technologies contain vulnerabilities and are not error free. Thus in all scenarios, the ‘victim’ may be incriminated or judged based on incorrect information and evidence, in that inaccurate or false behavioural patterns may be revealed. That is, a digital chronicle of an individual may not necessarily match the physical reality, and thus assumptions cannot be made without accurate contextual information and discussions. 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 implies deception and hidden agendas, which contribute negatively to social relationships. In cases where strangers are concerned, the issue is magnified and the psychological and legal ramifications are of primary importance. 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 minimise 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.

**Figure 2: Conceptualising the notion of covert policing within a community setting**

**References**


Myles, G., Friday, A. & Davies, N. (2003), ‘Preserving privacy in environments with location-based applications’, Pervasive computing, Published by the IEEE CS and IEEE Communications Society, pp. 56-64.