Emerging Forms of Covert Surveillance Using GPS-Enabled Devices

Roba Abbas, University of Wollongong, Australia

Katina Michael, University of Wollongong, Australia

M. G. Michael, University of Wollongong, Australia

Anas Aloudat, University of Wollongong, Australia

EXECUTIVE SUMMARY

This case presents the 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 case investigates five stakeholder relationships using scenarios to demonstrate the potential socio-ethical implications that tracking and monitoring will have on society. The five stakeholder types explored in this case include: (i) husband-wife (partner-partner), (ii) parent-child, (iii) employer-employee, (iv) friend-friend, and (v) stranger-stranger. Mobile technologies like 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. Limited laws and ethical guidelines exist for members of the community to follow when it comes to what is permitted when using unobtrusive technologies to capture multimedia and other data (e.g., longitude and latitude waypoints) that can be electronically chronicled. In this case, the evident risks associated with such practices are presented and explored.

Keywords: *Behavioral Tracking, Breadcrumb, Covert Surveillance, GPS, Location-Based Services, People, Relationships, Scenarios, Smart Phones, Socio-Ethical Implications, Trust*

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 iden-

DOI: 10.4018/jcit.2011040102

tification (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 have become 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 serious socio-ethical consequences. This case 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 case 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 case.

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 case, 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 case 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.