00

Privacy implications of automated GPS tracking and profiling

Muhammad Usman Iqbal
PhD Candidate, School of Surveying and Spatial Information Systems, University of New South Wales

Samsung Lim
Senior Lecturer, School of Surveying and Spatial Information Systems, University of New South Wales

Abstract

Recent advancements in GPS technology have opened new avenues for its use in the automotive sector. While GPS is a self-positioning system and does not threaten 'locational privacy', its availability in telematics systems enables various privacy abuses both in real-time and retrospect. GPS devices are being used for surreptitious monitoring, for providing alibis and more recently, by the government to access telematics-generated GPS data for complementing their mass surveillance projects. While researchers have presented theoretical studies of privacy abuses and their countermeasures, limited research has been conducted to assess these threats in a real-life scenario involving data obtained from people. This paper aims to raise awareness about privacy issues created as a result of GPS-based surveillance by conducting an experiment involving collecting positional data from a number of volunteers. A software protocol is implemented which takes this GPS data as input and produces profiles of road behaviour, social activities and work activities of the volunteers. Interviews are conducted with the volunteers to assess the accuracy of this profiling. Results suggest that while these profiles can be highly predictive of personality traits, they may also be misleading due to technical limitations and inaccuracies. Positional data is highly detailed and it is important to negotiate the function, storage and use of such data so that future telematics systems do not impinge upon privacy rights of motorists.

Keywords: Surveillance, location privacy, data-mining, threats, GPS, ethics, profiling, location tracking

1 Introduction

The automobile has gradually evolved from an analogue machine with mostly mechanical and hydraulic components to an electronic system with a growing number of computer-based

systems. Within the realms of this ‘smart car’ revolution, GPS vehicle navigation has attracted significant attention from consumers. It is generally accepted that the automotive industry would be one of the largest consumers of GPS technology. There are efforts already underway to use this infrastructure for additional value added services, for instance, mobility-pricing of insurance (Tripsense 2007; Norwich Union 2007), infrastructure-less electronic toll collection and GPS-enabled parking fee collection (Grush 2005).

These applications would require disclosure of positional data by its users in real-time through a communications infrastructure. These systems would process the positional data to charge the motorist for the services rendered. A decrease in the cost of electronic storage means that this captured data intended for a specific purpose, originally transaction processing, may be retained indefinitely or at least for long periods of time. Since GPS data is information rich, the temptation to use it for secondary purposes may be too great to resist.

While theoretical research has aimed to raise awareness about these threats and proposed algorithms to protect the privacy of individuals in location contexts (Gruteser & Grunwald 2003; Duckham & Kulik 2005), limited research has been conducted to assess these threats in a real-life scenario involving data obtained from people. This paper aims to raise awareness about privacy issues created as a result of GPS-based surveillance by conducting an experiment involving collecting positional data from a number of volunteers. A software protocol is implemented which takes this GPS data as input and generates a range of personal information about the individual including their home addresses, social and work activities. The next section explores pertinent issues in the ethics of GPS and society, followed by a detailed explanation of the research study.

2 Background

2.1 GPS alibi and GPS-enabled surveillance

There have been instances where motorists have successfully challenged issuance of speed tickets against them by providing their GPS data as evidence. These cases have set a legal precedent to question the accuracy of hand-held radar guns (Wainright 2007). Even navigation equipment manufacturers are taking this opportunity to market their products as potential ‘alibis’.

In other instances, legal precedents have also been set where the surreptitious installation and monitoring of GPS tracking devices does not require court orders (McCullagh 2005). The court ruled that the motorist has no expectation of privacy on a public roadway and it was legitimate for the police to perform surveillance of the vehicle without requiring a warrant. While warrants are not hard to acquire, they offer some judicial oversight where law enforcement personnel have to contact a neutral magistrate or judge and justify their suspicions when engaging in the tactic of surveillance, preventing abuse of the system.

Yet again, manufacturers are cashing in on the opportunity by advertising their tracking devices for covert surveillance operations, e.g. for curious spouses and employers. As shown in figure 1, some manufacturers even explain graphically how to covertly install these devices (TrackStick Pro 2007). These ethical issues require the attention of researchers and policy-makers to provide rigorous ethical safeguards on GPS tracking procedures.

Additionally, whether used as an alibi, or to convict somebody of a crime, GPS data is not suitable in its current form as evidence (Michael, McNamee & Michael 2006). The reason is that GPS devices lack any cryptographic protection for the tracks, routes and waypoints stored on its memory, and a compatible software tool can be easily used to edit the positional data. Unless there are cryptographic techniques present to digitally sign the contents for non-repudiation, innocent people can be framed and convicted, and traffic offenders would escape paying for fines.

Figure 1: Covert installation of GPS tracking device

2.2 Mobility-pricing and überveillance

Mobility-pricing of insurance is a new approach that employs location technology allowing for the customisation of insurance premiums to more accurately reflect the risks based on actual vehicle usage. This would reduce the cross-financing of high risk drivers by low risk ones and increase fairness of insurance systems. There have been successful pilot studies conducted throughout the world that use GPS and telematics technology to offer actuarially accurate insurance products (Tripsense 2007; Norwich Union 2007). In the Australian context, a recent statement by an NRMA (National Roads and Motorists' Association) Insurance official lauded the benefits that GPS-based insurance would offer to motorists but also acknowledged the inherent "Big-Brother-ish" qualities that such a product would bring about (NRMA 2007).

GPS logs are a form of data, and its monitoring would fall within the realms of informational surveillance. "Dataveillance", a term coined by Clarke (1988) refers to the use of personal data in monitoring actions of communications of individuals. M.G. Michael's work gives rise to the emerging notion of "überveillance", an above and beyond almost omnipresent surveillance system (Michael et al. 2006). It is possible that mobility-based insurance would conveniently enable this pervasive surveillance and potentially have a chilling effect to the privacy rights of motorists. These issues would be further aggravated by the government's interest in acquiring this data from insurance providers by offering them incentives. There is already speculation about this practice in the UK where an insurance company that offers mobility-pricing has been contacted by the government for data access for its own congestion charging scheme (Hytch 2007) in exchange for certain benefits. These developments, however, have not gone unnoticed by privacy researchers. Coroama and Langheinrich (2006) implemented a GPS based insurance system which calculates premiums on-board the vehicle guaranteeing privacy of owners. In this system, there is periodic transmission of aggregated information to the insurance provider for bill generation. Iqbal and Lim (2006) extended this idea further and proposed a GPS-based insurance product that preserves location privacy by computing distances travelled on the on-board unit and additionally safeguarded "spend privacy" by proposing smart card based anonymous payment systems.

2.3 Privacy in public

As mentioned in section 2.1, public surveillance has become a part of a modern citizen's life. The ubiquitous presence of surveillance cameras, speed cameras and electronic toll collection booths digitises and stores the movement of motorists on various databases. Motorists relinquish the right to privacy to obtain the privilege of using the road networks. That is why 'Privacy in public' is a difficult concept to grasp. Past research and legislation has focused on the old adage, 'A man's home is his castle', and has aimed to characterise privacy as a notion to protect an individual's right in their homes against unreasonable searches and seizures (Krull, 1999). Not much attention has been given to the notion of 'location privacy'. However, with emerging technologies that depend on GPS for their data processing, it is vital that adequate attention is paid to building a theory of privacy in public by drawing from existing legal frameworks and philosophical contexts.

Nissenbaum (2004) proposes the theory of 'contextual integrity' to tackle the complex issue of privacy in public. This theory is built around the notion that all realms of life are governed by norms of appropriateness and norms of distribution. Norms of appropriateness distinguish between intimate information that is appropriate to disclose and information that is inappropriate. Likewise, norms of distribution govern how personal information about somebody is shared with others. While norms of appropriateness would allow one to discuss relationship problems with a close friend, the close friend would be violating the norms of distribution if s/he discloses this information to a third party. Contextual integrity is maintained when both the norms of appropriateness and norms of distribution are respected.

3 Research Motivation

3.1 Related Work

Location is an important aspect of context in pervasive computing, and has attracted considerable attention from researchers to extract "significant locations" from positional data. Signification locations may be the residential address, places of interest for an individual including preferred shopping centres or restaurants. Ashbrook and Starner (2003) used GPS data from a single volunteer collected over a four month period and used it to derive the locational context of a user. They developed an algorithm which extracted significant locations from the GPS data and used it to design an intelligent predictive model of the user's future movements.

Krumm developed a similar protocol and tested it to identify the home location and infer identities of the volunteers. He collected the data from 172 individuals and used a reverse geo-coder to infer home locations of roughly 5% of the participants correctly. He then applied the theoretical countermeasures already present in location privacy research, such as spatial cloaking (Gruteser & Grunwald 2003), noise and rounding (Agrawal & SriKant 2000) on the GPS data and tested their effectiveness by quantifying how well these algorithms prevented the inference algorithms from finding the subjects' home addresses.

Michael et al. (2006) used a combination of GPS receiver data and diary logs of a volunteer over a period of two weeks to seek an understanding of the social implications of tracking and monitoring subjects. Their research identifies the ethical dilemmas associated with use of GPS on civilians and points out that adequate safeguards need to be placed to avoid abuse of information gathered through GPS technology.

In terms of driving behaviour, Greaves and De Gruyter (2002) discuss how a driving profile of a person can be derived from GPS track data. They sought an understanding of driving behaviours in real world scenarios by fitting low-cost GPS receivers to vehicles, and logging the

vehicle movements. Consequently they were able to identify driving styles from this data.

3.2 Motivation

Previous sections have set the theoretical stage for conducting a privacy assessment of GPS tracking. This paper is one of the first efforts to collect and analyse location data from multiple volunteers and generate automated profiles without human intervention. This motivation comes from the fact that it would be cumbersome to analyse GPS data of a large number of individuals on a manual basis.

The attack model simulates a typical adversary's three main moves. The first step is information collection using passive surveillance. This step is followed by information processing by using data-mining, pattern recognition, and reverse geo-coding of significant locations. Finally in the third step, the adversary performs information dissemination by creating summary profiles.

4 Research study

4.1 Surveillance

In order to mimic truly surreptitious surveillance, a GPS tracking device was required that worked without any input and intervention from the users. The selection process led to choosing a passive GPS device known as the Trackstick Pro as shown in figure 2. This GPS stick uses power from the cigarette lighter in the car and has a memory of 4 megabytes, which is suitable for storing the track data for up to a period of one month.

Figure 2: The GPS device used

Figure 3: Installed and operational

A total of five volunteers were selected for this study. The sample consisted of an undergraduate student, a research student, an academic staff member, and two support staff from the school. Before the study began it was hypothesized that different types of people would have different patterns, so a sample space was drawn that represented the different communities at the university. As shown in figure 3, volunteers were shown how to attach the GPS stick to their vehicle's dashboard using double sided tape and the cigarette lighter plug in the cigarette lighter jack. The GPS device had to be placed such that the globe would face up, as shown in figures 2, and 3. The volunteers were advised not to remove the stick or the power source for the period of study. At least one week's worth of data was collected from all the volunteers. The sticks were circulated and collected on Wednesdays to include both weekend and weekday driving. It was

expected that the passive nature of the device would yield data closest to the actual driving attitude of the volunteers and would not result in behaviour modification on their part.

The GPS device was configured to be used in a vehicle through the software drivers present on the PC (Personal Computer). On the average it logged location, time, date, speed, elevation and temperature data at a rate of 6 times per minute. Although the desired logging rate would have been on a per second basis, the TrackStick is not capable of logging at such a high rate. Ultimately, this option was chosen as a trade-off between granularity and convenience for the volunteers. On completion of the specified period, the GPS data was downloaded to the PC and stored anonymously without identifying the volunteer in any way.

4.2 Information Processing and dissemination

4.2.1 Home and work location identification

The first step in the analysis is to identify significant locations from the data. As shown in figure 4, the GPS device logs the status as "Power Off" when the ignition of the vehicle is switched off. The data row prior to this event (marked with a red circle) has a significant location since this is the last known position before the vehicle stopped. Note that the speed for the record is not zero as the tracking device roughly logs around 6 times per minute. This means that the actual parking position can be metres away. This inaccuracy requires softening the location identification algorithm and including a buffer of 4 properties around the one that the solution finds to be the valid address of the volunteer.

Rec #	Date	Time	Latitude	Longitude	Altitude	Status	Course	GPS Fix
134	03/17/2007	11:15	-33.9120°	151.1194°	24.7 m	31 kph	NE	Y
135	03/17/2007	11:15	-33.9116°	151.1199°	25.4 m	31 kph	NE	Y
135	03/17/2007	11:15	----	----	----	Power Off	----	----
140	03/17/2007	11:22	----	----	----	Power On	----	----
141	03/17/2007	11:22	-33.9054°	151.1275°	0.0 m	0 kph	N	Y

Figure 4: GPS track data downloaded onto PC from GPS device

The algorithm is implemented in Visual Basic.net. The purpose of choosing this programming language is that there are APIs (Application Programming Interfaces) available in this language that would programmatically allow connecting to the GIS (Geographical Information System) software for further analysis and profiling. The algorithm selects all the locations prior to the "Power Off" signal in an effort to identify the home locations. Since all the volunteers are associated with the university, the algorithm does not compute the work locations and concentrates in identifying home locations only. The algorithm uses certain heuristics so that on weekdays, it is weighted to give higher importance to significant locations during the period between 3 PM – 10 PM. This rule is based on the fact that most people's trips would end at their home locations during this time period.

To find the nearest street address to the significant locations, PSMA (Public Sector Mapping Agencies) Australia's GNAF (Geo-coded National Address File) index is used. This address file contains the geocode (specific latitude and longitude) of all physical addresses in Australia. This data is stored in a spatial database capable of performing spatial queries. PostGIS which spatially enables the PostgreSQL database server is used to store the GNAF data, since it is open-source and reliable to use. Due to the magnanimity of storage requirements, GNAF data for only New South Wales is loaded into the database which requires 5 gigabyte of storage space alone.

Home location	Volunteer C	Volunteer B	Volunteer Y	Volunteer J	Volunteer U
Street number(s) inferred	7	39	24, 25	44	53
Actual street number	11	39	22	Different street	51

Table 1: Protocol output of inferred home locations with actual addresses obtained from interviewing volunteers.

Using Spatial SQL (Structured Query Language) the filtered significant positions (through time heuristics) are queried from the database. The output is a set of physical addresses. The statistical mode is used to short-list the physical address of the volunteers. Since the mode is not necessarily unique, the physical address computed by the protocol may be more than one. Table 1 summarises the protocol output at this stage. Only initials of the volunteers are used to keep their details anonymous. For Volunteer B, the inferred address was the actual street address. For three out of the remaining four volunteers (C, Y, U), the physical address computed was the next door address where they actually lived, which according to the assumption falls within the 4 address buffer range. For Volunteer J, the physical address computed was on a parallel street. The logical explanation for this is that the volunteer parked his car in an underground car park and entered the street through a parallel street so the last significant position is recorded on the road closest to the proposed street address as shown in figure 5. The volunteers were shown a list of all the computed addresses and asked to find out the closest one to their address.

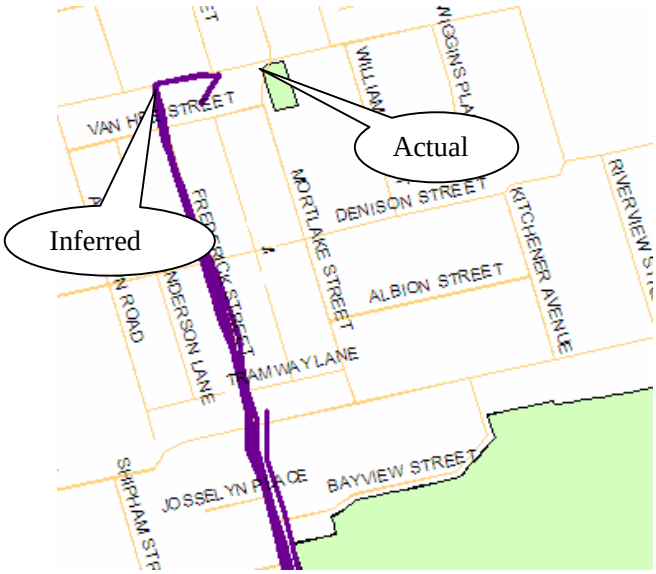

Figure 5: Street address for volunteer incorrectly guessed by the home determination algorithm

4.2.2 Profile generation

After inferring the street address of the drivers, the next stage is to use the same data and make inferences about their social and work related activities. The whole GPS track data is sifted and aggregated, and the output of this step is summarized in table 2. While this list is not exhaustive, it is evident that a lot of calculated guesses can be made about individuals based on this data. Inferences can be drawn about how long a person spends time at work, and what times the person is not at their home. This information can be used by adversaries with malicious intent. Krumm (2007) has furthered this idea and computed relative probabilities of the times when a subject may be home. Additionally the speed and travelled distance details indicate how long a person stays on the road and the average distance travelled each day.

Work and commute profile	Volunteer C	Volunteer B	Volunteer Y	Volunteer J	Volunteer U
Total GPS records	5240	1997	2330	4812	2147
Total Distance	301 km	174.59 km	172 km	284.9 km	149.72
Average distance	27.38 km	34.59 km	31.2 km	40.7 km	37.43 km
Total travel time	12 hr 45 m	4 hr 25m	5 hr 1 m	11 hr 44 m	4 hr 51 m
Average travel time	1hr 10 m	52 m	54 m	1 hr 40 m	1 hr 12 m
Max Speed	101 kph	83 kph	86 kph	98 kph	91 kph
Average Speed	32 kph	45 kph	39 kph	33 kph	39 kph
Average time leaves home	7:33 am	8:21 am	9: 10 am	07:46 am	9:54 am
Average time leaves work	3:30 pm	5:09 pm	4:54 pm	08:58 pm	5:07 pm
Average time arrives at work	8:03 am	8:55 am	9:32 am	08:40 am	10:15 am
Average time at work	7 hr 58 min	8 hr 10 min	7 hr 25 min	12 hr 18 m	6 hr
Parks car in	University parking lot	University parking lot	University parking lot	University parking lot	Around university
Type of person	Academic Or Support	Academic Or Support	Academic Or Support	Research Student	Undergrad Student

Table 2: Profile summary of volunteers generated by the software protocol

Volunteer Y seems to spend the longest time at the university, and lives the farthest distance. On average he/she has to travel approximately 40 kms to commute to work and back home each

day. The algorithm is also designed to guess the profile type of the individual with the GPS. For example, a rule that is incorporated in the protocol is that a person spending a great amount of time at university is most likely a research student. Likewise, a person who has a vehicle and does not park at the university parking lot is not privileged with a parking permit. Another heuristic used is that if a person parks within 1 km buffer around the university, then he/she does not have a parking permit and is most likely an undergraduate student. While these heuristics have proven to be true in this particular case, they may not necessarily always be valid. For instance, there might even be an academic staff member who is putting in extra hours to prepare lecture material for the forthcoming semester. Under the present algorithm, he/she would be identified as a research student.

Further inferences can also be drawn using this data to determine social networks, for instance Wigan and Clarke (2006) have highlighted issues related to location tracking and social networks. They argued that continuous tracking of vehicles can produce trails which can tell where a person currently is. This information can be correlated to another person's location at the same time to probabilistically infer social networks. Additionally, the routes that a person takes to reach different destinations can also provide crucial information to their individual pattern.

4.2.3 Driver behaviour analysis

In this section speed and acceleration analysis is carried out. While the algorithm produced speed and acceleration graphs, as well as speed maps for all the volunteers, for the sake of clarity and brevity, only one volunteer's data is discussed.

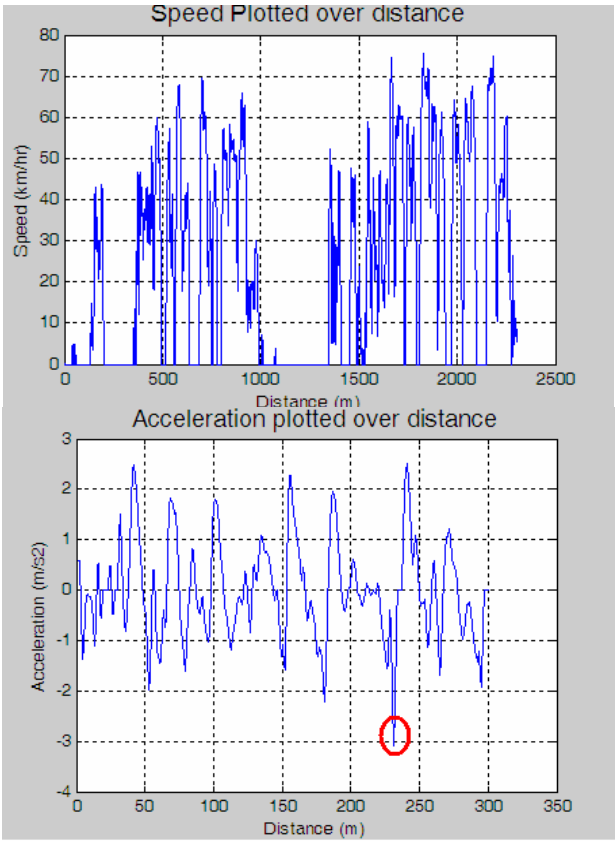

Figure 6: Speed and acceleration graphs for volunteer

Intuition suggests that individual driving behaviour is a function of many factors such as characteristics of that individual, for instance, the driver's age, gender, purpose of trip, the type of vehicle and reported traffic conditions. It is also widely acknowledged that higher speeds increase the likelihood and severity of collisions (Kloeden et al. 1997). The purpose of this section is to demonstrate that GPS data can be used to make inferences about an individual's driving behaviour. This road activity analysis was carried out by generating speed and instantaneous acceleration graphs as well as detailed speed maps of trip data where speed variability is represented using different colours on GIS maps. As mentioned earlier, VB.net was used to programmatically access the GIS APIs for dynamically constructing the required maps of speed data. The road network data was obtained from PSMA's "Transport and Topography" dataset. This dataset was in MapInfo format, and had to be converted to ESRI compliant format using a freely available conversion tool.

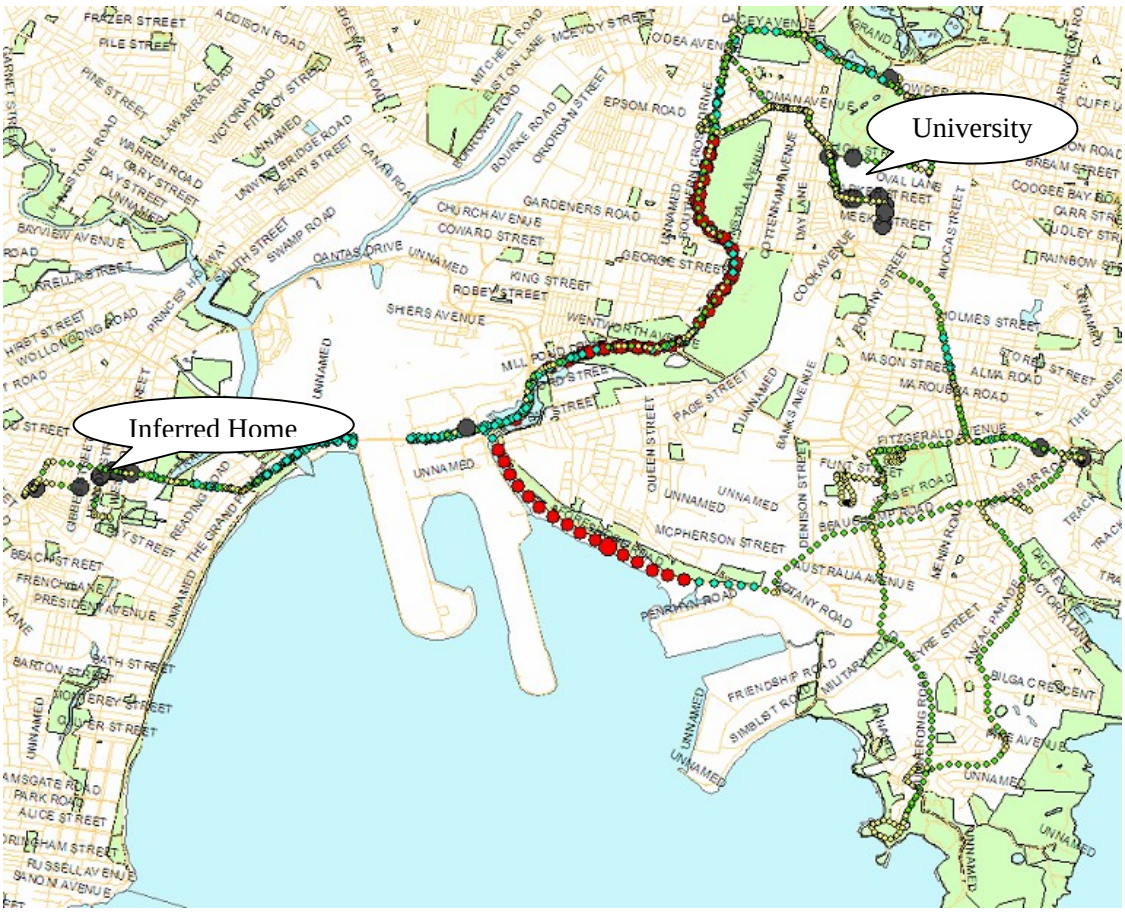

Figure 7: Speed profile of volunteer using waypoint data

In this stage, the GPS data was programmatically converted to ESRI Shapefile format, which is the preferred file format for ArcGIS. Version 9.2 of ArcGIS was used. All the records from the GPS data that had a status of "Power On" were removed as they had no positional information and could not be used on the map. The points with the "Power Off" status were edited in this process to have positional information of its preceding GPS record. These would prove useful in demonstrating the idea of significant locations mentioned in the location identification section. The resultant output was two sets of Shapefiles, one for the GPS track and the other for GPS

waypoints respectively.

Figure 6 shows the speed and acceleration graphs plotted for a particular volunteer. It can be observed in the acceleration sub-graph that the individual had to decelerate the vehicle at -3 m/s^2 at a certain stage, which is considered risky according to prior research (Watson 1995; Greaves & De Gruyter 2002). In terms of environmental impacts, even though the impact of overall driving styles may be less obvious, high speeds (80 kph and above), rapid accelerations and decelerations of more than +/- 3 m/s^2 are considered to be a source of increased fuel consumption and emissions and may indicate the driving behaviour of individuals.

Figure 7 represents the routes the individual took from the home location to the university. The black dots on the map indicate significant locations that were used to infer home locations. Note the black dots around the university vicinity, where the volunteer had parked the car frequently and were used to predict if the volunteer was an undergraduate student. The red dots indicate that the speed with which the car was being driven was greater than 80 kph. With access to speed data of all the roads, it can be easily correlated to find if an individual was over the speed limit. It is also not hard to imagine that if insurance companies get access to this data, they would use this information, in order to identify an individual with an 'aggressive' driving style. The insurance provider can then assign the individual a higher risk, leading to a higher premium or denied motor insurance altogether (Iqbal & Lim 2006).

5 Discussion

Using an adversarial attack paradigm, the protocol involved information collection using surveillance, information processing using data-mining and information dissemination using spatial maps and tabular reports. The profiling exercise looked at various aspects of the volunteers' lives and predicted what class of personnel they belong to (academic staff, support staff, graduate student or undergraduate student). The protocol also identified the residential address of 4 out of 5 volunteers within the specified spatial granularity. The protocol further characterised the road behaviour of volunteers by looking at speeds and accelerations.

While results suggest that these profiles can be highly predictive of personality traits, they may also be misleading due to various reasons. For instance, one of the heuristics used was that the person spending the most time at university is most likely a graduate student. Spending more time at the campus doesn't necessarily mean that one is at work. A student may be involved in extra-curricular activities or work on campus cafes and bookshops. Similarly, an academic may be on campus for extended periods of time preparing lectures for the forthcoming semester or applying for a research grant.

Future telematics applications would work on location data in order to provide services. For instance mobility pricing of insurance (Norwich Union 2007), which brings the concept of "fairness" to insurance premiums would require disclosure of positional to generate per-mile premiums. However, there would also be unintentional transmission of data that may be used against the motorist, for instance how hard one brakes/accelerates or how often one goes above the speed limit. One solution to avoid these abuses is to aggregate the GPS data and send only the information necessary for premium calculations. A similar privacy-aware system recently identified is the GM FleetView (2007), which is primarily for fleet management, but has built-in privacy features. Employees may find such systems quite useful to track work-related travel for tax purposes; however, these individuals operating such vehicles have a reasonable expectation of privacy when using the vehicles after-hours. This system has a toggle switch in the vehicle which an employee can select to identify a business or personal trip. Location of the vehicle would not be transmitted when driving in personal mode. To conclude, it is imperative that future telematics systems respect the privacy of motorist and provide configurable features for motorists to opt-out or opt-in on a more granular scale.

6 Conclusion

The purpose of this experiment is to demonstrate that GPS data can be used to draw numerous inferences about individual personality traits by a simple click of a button. These inferences can be used to harm an individual and may prove embarrassing to him/her when revealed publicly. Future invasions of privacy in location contexts would employ technologies presented in this paper. With the recent trend of installing GPS chips in mobile phones in order to accessorize them with navigation features (Roche 2007), one should ask what safeguards have been provided that mobile phones cannot be remotely hacked to gain access to this data? With accounts of law enforcement officials remotely activating mobile phones of suspects for audio surveillance (McCullagh & Broache 2006), it is not hard to imagine that the GPS data could also remotely and surreptitiously be read providing a ubiquitous surveillance device. The combination of motorists and mobile phone users form a huge majority of the urban population and citizens should not be victims of mass surveillance or privacy abuses based on location data. Rigorous ethical and legislative safeguards need to be implemented to protect future abuses of individuals' privacy in this context. Location technologies are still in their nascent stages, therefore, from a technology point of view, it is important to dispel these privacy concerns right from the beginning, and focus on "building in" privacy protection within such systems so that as new applications become available, appropriate privacy measures are integral to them.

Acknowledgements

The author wishes to acknowledge the financial assistance provided by the 'Metadata Scholarship' from OMNILINK Pty. Ltd. for this research.

References

Agrawal, R & Srikant, R 200, 'Privacy-Preserving Data Mining', in ACM SIGMOD *Conference on Management of Data*. Dallas, TX, USA: ACM Press.

Ashbrook, D & Starner, T 2003, 'Using GPS to Learn Significant Locations and Predict Movement across Multiple Users', *Personal and Ubiquitous Computing*, 2003. 7(5): pp. 275-286.

Clarke, RA 1988, 'Information Technology and Dataveillance', *Communications of the ACM*, 31(5),1988, pp. 498-512.

Coroama, V & Langheinrich, M 2006, 'Personalized Vehicle Insurance Rates – A Case for Client-Side Personalization in Ubiquitous Computing', Paper presented at the *Workshop on Privacy-Enhanced Personalization* at CHI 2006, Montréal, Canada, 22 April, 2006.

Duckham, M & Kulik, L 2005, 'A Formal Model of Obfuscation and Negotiation for Location Privacy'. *Lecture Notes in Computer Science*, 3468, pp. 152-170.

GM Fleetview 2007 GM FleetView Presentation Video, viewed 18th March 2007, http://video.vividas.com/media/4630_GMFleet/web

Greaves, SP & De Gruyter, C 2002, 'Profiling driving behaviour using passive Global Positioning System (GPS) technology' presented at *Institute of Transportation Engineers International Conference*, Melbourne, Australia.

Grush B 2005, 'Optimizing GNSS-Based Mobility Pricing for Road-Use, Parking, and PAYD Insurance', *4th European Traffic Congress*. Salzburg, Austria

Gruteser, M & Grunwald, D 2003, 'Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking', Paper presented at the *First International Conference on Mobile Systems, Applications, and Services*, San Francisco, USA.

Hytch D 2007, 'Service vendors target traffic-management deals', *Computer Business Review Online*, viewed 25 July 2007, <http://www.computerbusinessreview.com/article_news.asp?guid=E01E9184-2F51-4B85-9577-D0A6C72AF895>.

Iqbal, MU & Lim, S 2006, 'A privacy preserving GPS-based Pay-as-You-Drive insurance scheme', *Symposium on GPS/GNSS (IGNSS2006)*. Surfers Paradise, Australia, 17-21 July, CD-ROM proceedings.

Kloeden, CN, McLean, AJ, Moore, VM and Ponte, G 1997, 'Travelling speed and the risk of crash involvement', *Report CR 172*. Federal Office of Road Safety, Canberra.

Krull, K 1999, *A Kid's Guide to America's Bill of Rights*, pp. 224, New York, Avon Books.

Krumm, J 2007, 'Inference Attacks on Location Tracks', *Fifth International Conference on Pervasive Computing (Pervasive 2007)*, May 13-16, 2007, Toronto, Ontario, Canada.

McCullagh, D 2005, 'Snooping by satellite', *CNET News*, viewed 29 July 2007, http://news.com.com/Snooping+by+satellite/2100-1028_3-5533560.html

McCullagh, D & Broache, A 2006, 'FBI taps cell phone mc as eavesdropping tool' , *CNET News*, viewed 10 April 2007, <http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029_3-6140191.html >

Michael, K, McNamee, A & Michael, MG 2006, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring', in Proceedings of the *International Conference on Mobile Business*, Copenhagen, Denmark, 25-27 July 2006. IEEE Computer Society.

Michael, K, McNamee, A, Michael, MG & Tootell, H 2006, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS', in Proceedings of the *International Symposium on Technology and Society*, New York, 8-11 June 2006. Copyright IEEE Computer Society.

Nissenbaum, H 2004, 'Privacy as contextual integrity', *Washington Law Review*, 79 (1), 119-157.

NRMA 2007, 'NRMA calls for car surveillance via GPS', *Ninemsn Science and technology news*, viewed 10 July 2007, <http://news.ninemsn.com.au/article.aspx?id=59964>

Norwich Union Pay As You Drive Car Insurance, viewed 5 June 2007, <http://www.norwichunion.com/pay-as-you-drive/index.htm>.

Roche, J 2007, 'Nokia N 95', *CNET News*, viewed 28 July 2007,<http://www.cnet.com.au/pdas/gps/0,239035573,339271384,00.htm>.

TrackStick Pro, TrackStick Pro userguide, pp 30, viewed 12 April 2007, < http://www.trackstick.es/files/STS_user_guide.pdf >

Tripsense, How TripSensor Works, viewed 11 January 2007, <https://tripsense.progressive.com/about.aspx?Page=HowDeviceWorks>

Wainright R 2007, 'Father and son stick to gins to prove radar wrong', *Sydney Morning Herald*, viewed 5 July 2007, <http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html>

Watson, HC 1995, 'Effects of a Wide Range of Drive Cycles on the Emissions from Vehicles of Three Levels of Technology', *Global Emissions Experiences*, SAE, Warrendale, Pa., USA. SP-1094,p119-132.

Wigan, M & Clarke, R 2006, 'Social Impacts of Transport Surveillance', *Prometheus*, 24, pp. 389-403.

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.