



**International Global Navigation Satellite Systems Society
IGNSS Symposium 2006**

Holiday Inn Surfers Paradise, Australia
17 – 21 July 2006

A Privacy Preserving GPS-based Pay-as-You-Drive Insurance Scheme

Muhammad Usman Iqbal

School of Surveying and Spatial Information Systems,
The University of New South Wales, Sydney NSW Australia
Tel: +61 2 9385 4206 Fax: +61 2 9313 7493 Email: m.iqbal@student.unsw.edu.au

Samsung Lim

School of Surveying and Spatial Information Systems,
The University of New South Wales, Sydney NSW Australia
Tel: +61 2 9385 4505 Fax: +61 2 9313 7493 Email: s.lim@unsw.edu.au

Presenter Name: M.U Iqbal

ABSTRACT

The emergence of low cost GPS receivers has spurred the development of an increasing number of satellite-based positioning applications. In the automobile industry, satellite-based positioning offers promising services. One such application is Pay-as-You-Drive (PAYD) insurance. The aim is to design mobility-based insurance policies that would potentially reduce the premiums of car owners who do not travel often and/or long distances or are safe drivers. The premiums can be estimated by the total kilometres travelled, the zones where travel was made, the times of the day that the vehicle was used, and the average speeds. Although PAYD offers cost reduction for motorists, there are serious privacy concerns surrounding the application due to its ubiquitous tracking capability. The insurance providers can infer a lot more than just how many kilometres a motorist drove in a billing period. If tracking is continuous, they can estimate the risks of a particular driver being on the road, and how often, and of what nature, were offences made on the road. Ultimate control of location information should belong to the insured individual and has to be mandated through regulation or other means. Since PAYD is in its infancy, and no specific legislation exists, its acceptance depends on a technological solution that preserves

driver privacy. The authors propose a privacy preserving PAYD system that promises cost reduction incentives for the driver yet still safeguards their right to privacy. The paper presents the design of an onboard payment system that preserves driver privacy using anonymous digital cash for payment of insurance premiums. Real-time modelling of risk is proposed using an array of variables like onboard sensors, driving times, current road and weather conditions and onboard spatial databases with road risks and speed limits. These represent the actual risks faced on road and can be used to calculate policy premiums. Aggregated, anonymized and encrypted data is sent back to insurance provider for modelling of rating variables and quality control of current variables. The whole system ensures a measure of privacy by curtailing exchange of location information between vehicle and provider and implementing the payment system on the onboard vehicle computer.

KEYWORDS: Location privacy, Automobile insurance, GPS-based pricing, onboard payment systems, Privacy Legislation.

1. INTRODUCTION

In the automotive industry, satellite navigation is becoming increasingly available on new mid range car models as standard feature. Alternatively, aftermarket GPS navigation products are also becoming increasingly affordable and available. This capability permits the use of positioning equipment for other value added services. Researchers have recently started exploring opportunities of offering novel applications in the automotive sector by using positioning technologies. These range from emergency response systems, mobility based payment systems, electronic toll collection, satellite tracking of lost or stolen vehicles, satellite navigation, vehicular internet access, traffic monitoring, custom weather reports, parental vehicle tracking, remote prognostics and diagnostics (Grush, 2005; Vidales and Stajano, 2002; Zhang, Wang, and Hackbarth, 2003).

Due to socio economic activities attracting more and more people to larger metropolitan cities, there is a proportionate increase in road traffic. As a result, mobility based pricing of services has received recent attention to solve the issues of traffic congestion, increased pollution, increased parking costs, and increased accident rates (Vrhovski *et al*,2004). One such suggestion is to convert the fixed cost of motor vehicle insurance to a variable one based on the annual mileage. This class of insurance schemes are generally referred to as Pay-as-you-drive (PAYD) Insurance. The key idea here is to transform the “drive all you can” flat insurance premium to a mobility based paradigm. In such a design approach, the risk and premiums are modelled depending on the actual usage rather than approximation of future risks. This approach would give incentives to drivers for using the roads more efficiently and safely.

The classical motor insurance products work on statistical data by dividing the population into different risk classes based on long term demographics. The parameters used to model risk and design the payment equation use fairly static quantities like age and sex of driver, driving experience, residential post code, vehicle garaged or parked off street, vehicle’s safety equipment, intended vehicle use (business or pleasure), claims history (Athearn *et al*, 1989) . Cost of insurance depends on the future, there can only be predictions about the number of losses, their respective costs and times of occurrence. Actuaries designing traditional insurance policies do not have access to real-time risks faced by the motorists on road and thus cannot model these risks in premium calculations. This adversely affects the subset of

low risk drivers in a particular class who ultimately pay a higher premium the successive year due to the claims made by high risk drivers of the insured group. Researchers have argued about the actuarial inaccuracies of current insurance policy design (Litman, 2003). Therefore, the shift towards insurance products where prices reflect costs would be a natural one.

The technological developments in positioning and availability of mobile communications infrastructure have paved the technical feasibility for PAYD. Several insurance companies have launched pilot projects to market this idea. Currently these projects may focus on different market segments and adopt different approaches and variables for calculating premiums, but the general idea is to charge consumers based on mileage. Norwich Union (2006) in the UK was amongst the first insurance providers to market a GPS based pilot insurance product where the trips done by a vehicle were logged and then transmitted to the Insurance provider using the GSM network. Premiums were calculated on a monthly basis and invoices mailed out to vehicle owners. Their product focused on young drivers who pay higher premiums using classical insurance policies. Another possible design approach was taken by Progressive Insurance in the United States. Their product called TripSense did not use GPS to track the trips, but a device was used to register the time and day for each trip, the distance travelled, and speed. This system also kept track of hard brakings and quick accelerations. The insured person could download the data to a personal computer, and if satisfied, could upload this data to the insurance company's server at their discretion. Discounts of up to 25% were offered to drivers for volunteering for these insurance policies. This system motivated safe driving, and also gave incentive to drivers to use roads during off peak hours (TripSense, 2006).

PAYD is a business model of individualising insurance products. The aim is to get closer to the consumers using telematics services. Since there is exchange, storage and retrieval of precious personal spatial information, consumers can be very sceptical about the processing of their private information, especially location information, which can reveal a lot about an individual's personality traits. Using the aforementioned insurance products, specifically the ones that use GPS to locate and report the position data, there is a possibility of ubiquitous surveillance of individuals, both on a real-time and retrospective basis. Therefore, it is important to recognise and respect the driver's location privacy concerns if the insurance industry wants PAYD to be a successful business model. There is no privacy legislation that specifically covers the driver location privacy in using telematics services, and there is evidence that the corporate world is very good at obscuring questionable practices with fine print in a service agreement or contract (Schilit *et al*, 2003), therefore, it is essential to have a technological solution to safeguard driver privacy.

The purpose of this paper is two folds. The first is to propose a payment model where actual real-time risks encountered by a vehicle are calculated on an onboard computing unit. The authors do not discuss the exact specifics of a risk equation; this is better addressed in actuarial research. Payments for insurance premiums are debited from an electronic-cash smart card device, this guarantees location privacy of drivers as no location data is required to be transmitted to the insurance provider for payment processing. The second purpose is to exploit spatial databases, like speed limits of existing roads and risks attributed to these roads by insurance companies, coupled with onboard sensors, and GPS to enhance and transform the Pay as you drive insurance proposal to a "Pay how you drive insurance". It is the authors' opinion that this work would be a milestone in utilising spatial information and on board sensory devices to get full potential out of revolutionary insurance products. The only exchange of information from vehicle to the insurance provider is system status and

aggregated driving record with no identity information. The on board payment system using anonymous cash equivalents does not identify a particular individual making transactions and hence completely preserves the individual's privacy when using mobility based insurance.

2. BACKGROUND ON PRIVACY

2.1 General

Much of the literature pertaining to privacy refers to Westin's concise definition of privacy,

"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" (Westin, 1967)

In the context of automotive telematics, location privacy is a special case of privacy, relating to the privacy of location information of the vehicle, and therefore, the driver. Telematics applications are diverse in nature, but nearly all of them depend on vehicle location information. Various techniques exist for location information disclosure, mainly categorized into either being 'Self-positioning' or 'Remote-positioning'. In Self-positioning systems, the vehicle is either fitted with a GPS receiver or Dead-Reckoning system (based on one or more gyroscopes, a compass and odometer) to locate where it is on the road. Remote-positioning systems require a central site to determine the location of the vehicle (Drane and Rizos, 1997). The result is a set of coordinates (or position) of the vehicle expressed in relation to a reference frame or datum. Remote-positioning systems track, compute and retain the location information at the central monitoring site, which can be privacy-invasive if personal information collected for a purpose may be used for purposes other than the one it was originally collected for. Self-positioning systems inherently protect location privacy because they do not report the location of the vehicle to any other system. If, however, a self-positioning system (like GPS) reports a vehicle's location to a server through a communications channel, then it too poses a risk to the privacy of the individual.

Motorists' privacy varies greatly from the privacy of an individual at home. A driver can be followed and tracked by law enforcement officials or adversaries without knowledge. On suspicion, a driver can be stopped and searched by police personnel without requiring a warrant (Blumberg *et al*, 2005). Therefore, it is important to note that the most vital information about a driver is their identity and position with respect to time. Mapping, survey or Geodetic data has no personal information. However, when a person activates a GPS location device and this location information is reported and placed on a map, it becomes a personal map, and hence private information. Personal location information collected may be used for unsolicited marketing, locating people with malicious intent, or for creating personality profiles by behaviour on road.

2.2 Driver Privacy and Insurance

The main motivation to study privacy in the context of motor insurance is the work by Greaves and De Gruyter (2002). They 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. Imagine a PAYD insurance provider accessing 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, not to mention the capability of locating and tracking individuals in real-time or retrospect.

A fair idea of the requirements of a privacy preserving system can be determined by reviewing existing proposals for PAYD and their respective privacy factors. Three proposed systems are studied below and summarised in TABLE 1.

2.2.1 Odometer audits

The simplest form of PAYD is performing odometer audits. These can be done when a vehicle is serviced. Service personnel can be trained to check and validate the odometers and report them to the insurance agency securely. The insurance company can then readjust the premiums of the vehicle based on the kilometres driven. This method does not reveal any private information about the motorist, only the total kilometres driven in a financial year. Total kilometres of a vehicle are also used when trading cars, so it is not much of an issue. Besides, there are minimal infrastructural costs required to setup such a system.

2.2.2 Incentive based reporting of driving pattern

A second, richer approach is to have devices fitted to the vehicle, similar to the ones adopted for TripSense (2006) by Progressive Insurance. The times of the day the vehicle was driven can be recorded, and hard brakings and rapid accelerations are noted. It is at the discretion of the vehicle owner to view this data on computer, and if deemed appropriate, upload this to the insurance company's server to receive discounts and rebates on existing insurance policy. This type of a system requires more costs for setup as compared to the odometer based system. However, it has more information transmitted to the insurance company. The insurance provider can infer the number and durations of travel made during peak hours and off peak hours and regulate premiums accordingly. The driver is encouraged to use the vehicle more economically and, at the same time, help in problems like congestion and pollution. The number of hard brakings and accelerations can reflect information about the individual driver's behaviour on road. Therefore, there is more invasion of privacy compared to odometer based auditing, even though no real-time or passive information about the vehicle's location is transmitted.

2.2.3 GPS based mobility insurance

The last approach is a GPS based PAYD system. This class of systems transmit GPS logs to the insurance provider via a communications channel. Premiums are calculated by inferring kilometres driven and bills sent to drivers periodically (Norwich Union, 2006). This system requires a GPS and communications infrastructure in place. As discussed earlier, GPS is a self positioning system and becomes privacy invasive only when the GPS tracked data are transmitted to a malicious third party. Greaves and De Gruyter's (2002) work has already discussed driver behaviour profiling using GPS logs. Transmitted GPS logs can reveal a lot more about the individual than just calculation of kilometres driven. It can be used to record

the places of interest of the driver, determine the driver’s road behaviour, perform real-time or retrospective surveillance of individuals, and create personality profiles to market related products and services. These social concerns would defeat the technological and economical benefits PAYD promises. Therefore it is imperative to redesign PAYD with privacy built in to the system.

	Traditional Insurance	Odometer Audits	Incentive based approach	GPS based PAYD
Mobility based premiums	Not possible	Possible	Possible	Possible
Infrastructure costs	None	Low	Medium	High
Privacy invasion	Low	Low	Medium	High
Time of day risk assessment	Not possible	Not possible	Possible	Possible
Road based risk assessment	Not possible	Not possible	Not possible	Possible
Conditions based risk assessment	Not possible	Not possible	Not possible	Not Possible
Actuarially accurate	Inaccurate	Slightly better than Classical Insurance	Slightly better than Odometer Audits	Slightly better than Incentive based

Table 1. Comparison of insurance approaches and related requirements

2.3 System Requirements

The above discussion and summary concludes that the requirement is a Pay-as-you-drive Insurance product where the price of premium charged reflects costs. In spite of its privacy concerns, the GPS enabled system by far offers many flexibilities to policy designers. If a self positioning system also becomes a self payment system by calculating premiums on board, the flexibility to offer variable risks based insurance preserving privacy would be viable. Since, the insurance provider’s interest should solely be relative to billing of correct payments, there should be no interest in monitoring the movement of motorists. The consumers should not have to choose between accepting the loss of privacy and loosing out on service. The requirements are a privacy friendly design that eases the tension between contrasting interests of insurer and insured.

3. SYSTEM DESIGN

3.1 Assumptions

Before proposing a design fulfilling the requirements, it is appropriate to make certain

assumptions. The hardware used in the system is assumed to be tamper proof including the GPS receiver, the temperature sensors and light sensors. The specific equation that calculates the premium is provided by the insurance provider, along with a spatial database of risks and speed limits for roads.

3.2 Proposed Design

FIGURE 1 represents the proposed system design.

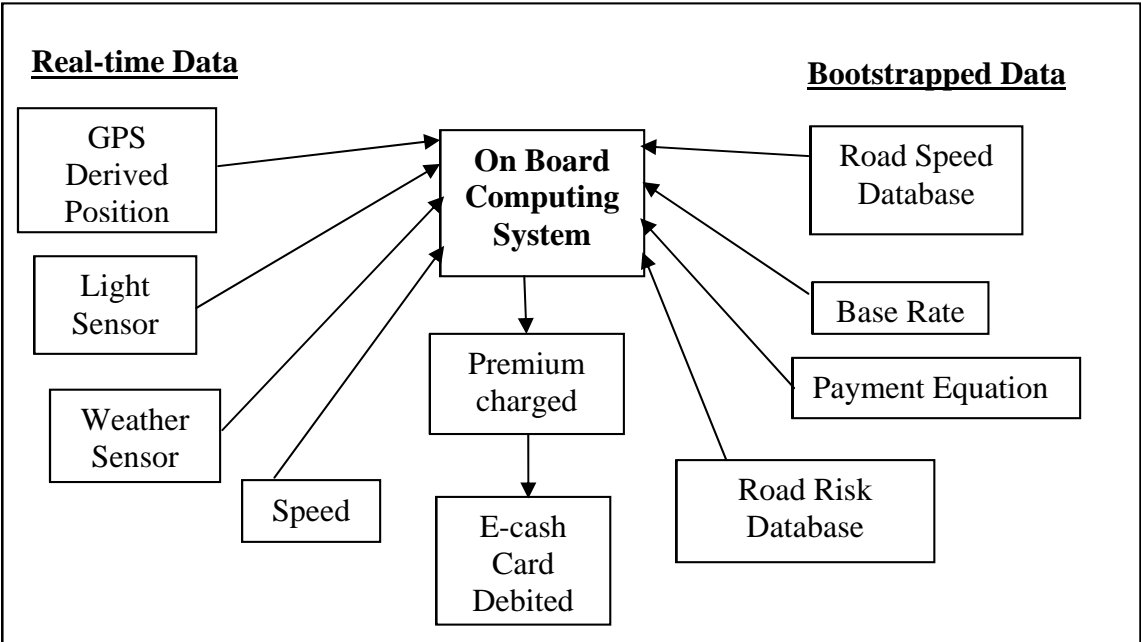


Figure 1. System Design: Bootstrapped data is provided by insurance company at policy set up time. The real-time data coupled with bootstrapped data is used by the on board computing system to calculate premiums debited from an e-cash smart card.

3.2 Real-Time Risk Assessment

Automobile manufacturers are fitting new cars with various sensors to improve the safety and reliability. Some of these sensors can depict the true risks that a motorist faces while driving. These include, but are not limited to, temperature, rain and light sensors, forward and rear distance sensors. Research suggests that driving in wet and dark conditions is more risky than driving on a sunny day (Litman, 2005; TripSense, 2006). Besides these sensors, the speedometer reports the driven speed continuously. To authenticate speed, the GPS receiver is also capable of estimating speed of the vehicle by simply taking two successive GPS positions in time. This can possibly be used to identify speedometer tampering.

At the time of setting up the policy, the insurance provider would collect information from the individual about their driving experience, claims history, age, sex, residential address, garaging location, year and make of vehicle, price insured for, security equipment fitted to the vehicle, any alterations made to the vehicle. This information would let the provider set up a base rate per kilometre for the premiums. The exact process of performing this calculation is beyond the scope of this paper. Assume the base rate is x Cents per kilometre.

The light and weather sensors report the light (dark or light) and weather (wet or dry) conditions to the on board computing unit for processing. The on board computing unit computes the weather conditions risk, termed WCR, and light conditions risk, termed LCR from these variables. There is a related risk table that is looked up to select a risk value for the reported light or weather variables. The light or weather sensors interact via a communications channel (infrared or Bluetooth) with the on board computing unit reporting a numeric value.

The GPS Receiver continuously reports the position, speed and time to the central computing unit. The reported GPS position data, coupled with current speed is checked with the roads database to find the current speed limit of the particular road stretch where the vehicle is travelling and whether the vehicle is over-speeding. The model also looks at curved roads and the speed on these roads. This is used to evaluate the speeding risk, SR. The GPS position is also used to query a road risks database to identify the current risk to travel on a particular stretch of road, this risk database is provided by the insurance company with extensive research related to accidents and high risk neighbourhoods. This particular risk is computed as road risk, RR. The on board computing unit attributes risks to the different received values and then loads them into the payment equation to calculate the premiums per second. The time and date quantities received by the GPS receiver from the satellite can be used to compute the time of day for assessing public holiday/weekend/weekday risks for the respective time, termed as rush hour risk, RHR.

$$\text{Premium/Second} = \text{Base Rate} * \text{WCR} * \text{LCR} * \text{RHR} * \text{SR} * \text{RR} \quad (1)$$

3.4 Anonymous Payment System

Digital cash or e-cash has been a prevalent concept on internet payment systems. There are mainly two types of e-cash systems, identifiable and anonymous e-cash. As the name suggests, the individual making the transaction can be identified by the bank in identifiable e-cash systems. The proposed system, however, uses anonymous digital payment to completely preserve the payment habits of an individual for insurance. The anonymous payment system uses blind signatures first proposed by Chaum et al (1990). This approach has been used efficiently, in internet based payment system, and preserves the identity of individuals making transactions.

At the time of policy setup, the insured individual is offered a smart card; the individual can top up credit to the smart card by a similar process of topping up prepaid mobile phones or phone cards. This smart card would have the aforementioned anonymous qualities of cash, i.e. secure and untraceable cash. Hypothetically speaking, these smart cards would be available to the individual from a pool of new smart cards. They would not require the identification of the individual; therefore, the identity of the individual cannot be ascertained from the smart card. The smart card can be inserted into a card reader on the vehicle's on board computing unit. The computing unit authenticates it to be a valid card, and checks if it has ample credit left. A threshold value can be set; reaching that value the system would continuously remind the insured individual of recharging the card to gain insurance.

The on board computing unit can keep track of when the vehicle was used without insurance and possibly can be used against the insured individual in case of a claim investigation is

made and is revealed that the vehicle was used uninsured. When queried by insurance personnel, the on board unit would only inform of the times and dates, if any, the vehicle was used with no insurance. This is analogous to driving the vehicle without renewing an insurance policy and is the individual's responsibility to maintain sufficient credit in the smart card. The payment mechanism used here is that of offline anonymous digital cash, this is the most complex form of e-cash. There can be scenarios of "double spending" [give ref], since digital cash is nothing but a collection of bits. A malicious individual can top up a smart card with digital cash, make a copy of the card and try to use both for paying for insurance premiums. To handle this, the on board computing device would maintain a database of bits of digital cash received in past transactions so that when the copied smart card is used, the system denies insurance.

3.5 Data Exchange With Insurance Provider

Designing the payment and risk assessment system on-board tackles the issue of privacy and the transfer of personal location information. However, there must be adequate mechanisms to report the system status to the insurance provider. The on board computing unit would send a report the health of the system to the insurance provider periodically, normally on a daily basis. Public key cryptography is used for ensuring encrypted communication. All on board computing devices as well as the insurer entity have a public/private key pair. The public key of the insurer is used to send messages from the vehicle back to the insurer securely; this message is also digitally signed by the vehicle's system for non-repudiation. The only identity information used here is the registration number of the vehicle and does not use the location of the vehicle at any instance. In case the health message is not received by the insurer, this can initiate an enquiry if the system has malfunctioned and requires service or replacement.

The proposed model has no exchange of location information to compute premiums. However, there should be sufficient modelling data made available for the actuaries to determine new rating variables, as well as improve the quality of current rating variables, because automobile insurance is a continuous refinement process (Farid J, personal communication, 12 April, 2006). Statistical data that gives break-down for accidents and claims based on weather conditions, time of day, and peak/off peak periods would be modulated regularly, and the payment equation revised as a result. Readjustment of the payment equation would be performed at insurance renewal, since a commitment would have been given by the insurer for the contract period. Therefore, for this reason, a periodic transfer of anonymized and aggregated data with no identification details is performed.

4. CONCLUSION

The authors have discussed the importance of preserving driver privacy in Pay-as-you-drive insurance schemes. The design of a privacy aware PAYD is presented by implementing the payment system on an on board computing device. This PAYD system is further enhanced and made more accurate by estimating real-time risks utilising spatial databases of road maps, real weather and temperature conditions and other road risks. In advocating consumer's privacy interests, a reasonable balance has been maintained by proposing a privacy respecting insurance model, with necessary analysis data provided to insurers. The next step is to develop an actuarially accurate payment system by collaborating with insurance experts and develop a prototype solution that can be installed on a vehicle and tested.

ACKNOWLEDGEMENTS

The authors wish to express their gratitude to Mr. Jawwad Farid from Alchemy Associates (Pvt) Ltd, a Fellow of Society of Actuaries, for the valuable input given in the design of the model. The authors also wish to express their sincere appreciation to the technical and financial contribution provided by OMNILINK Pty. Ltd for this research.

REFERENCES

- Athearn JL, Pritchett ST, Schmit JT (1989) *Risk and Insurance*, 6th edition, St. Paul, MN: West Publishing.
- Blumberg AJ, Keeler LS, Shelat A (2005) Automated traffic enforcement which respects "driver privacy", *Proceedings of the IEEE Intelligent Transport Systems Conference 2005*, Vienna, 941-946
- Chaum D, Fiat A, Naor M (1990) Untraceable electronic cash. *Proceeding of Crypto '88, LNCS 403*, pp. 319–327. Springer-Verlag.
- Drane C, Rizos C (1997) Role of Positioning Systems in ITS, In *Positioning Systems in Intelligent Transportation Systems* (pp. 298-299). Boston: Artech House, Inc
- Greaves SP, De Gruyter C (2002) Profiling driving behaviour using passive Global Positioning System (GPS) technology. Paper presented at the *Institute of Transportation Engineers International Conference*, Melbourne, Australia
- Grush B (2005) Optimizing GNSS-Based Mobility Pricing for Road-Use, Parking, and PAYD Insurance. Paper presented at the *4th European Traffic Congress*, Salzburg, Austria.
- Litman T (2003) Distance-based Vehicle Insurance. Victoria Transport Policy Institute.
- Norwich Union (2006). Pay As You Drive insurance. Retrieved 12 April 2006, from <http://www.norwichunion.com/pay-as-you-drive/>.
- Patiwat P (1996) Money in electronic commerce: digital cash, electronic fund transfer, and Ecash. *ACM Communications Magazine*, 39(6), 45-50.
- Sage A (2001) Future positioning technologies and their application to the automotive sector. *Journal of Navigation* 54: 321–8
- Schilit B, Hong J, Gruteser M (2003) Wireless Location Privacy Protection. *IEEE Computer Magazine*, 36(12), 135-137.
- TripSense (2006) TripSense-How TripSense Works. Retrieved 18 April 2006, from <https://tripsense.progressive.com/about.aspx?Page=HowDeviceWorks>.
- Vidales P, Stajano F (2002, September) The Sentient Car: Context-Aware Automotive Telematics, Paper presented at the *Location Based Services Conference 2002*.
- Vrhovski D, Moore T, Bennett L (2004) GNSS-based road user charging, *Journal of Navigation* 57(1): 1-13
- Westin AF (1967) In *PRIVACY AND FREEDOM* (pp. 7). New York: Atheneum.
- Zhang D, Wang XH, Hackbarth K (2003) OSGi Based Service Infrastructure for Context Aware Automotive Telematics, Paper presented at the *IEEE Vehicular Technology Conference*, Italy

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.