Location privacy in automotive telematics

Author:
Iqbal, Muhammad Usman

Publication Date:
2009

DOI:
https://doi.org/10.26190/unswworks/14892

License:
https://creativecommons.org/licenses/by-nc-nd/3.0/au/
Link to license to see what you are allowed to do with this resource.

Downloaded from http://hdl.handle.net/1959.4/44616 in https://unswworks.unsw.edu.au on 2023-10-26
Abstract 350 words maximum:

The convergence of transport, communication, computing and positioning technologies has enabled a smart car revolution. As a result, pricing of roads based on telematics technologies has gained significant attention. While there are promised benefits, systematic disclosure of precise location has the ability to impinge on privacy of a special kind, known as location privacy.

The aim of this thesis is to provide technical designs that enhance the location privacy of motorists without compromising the benefits of accurate pricing. However, this research looks beyond a solely technology-based solution. For example, the ethical implications of the use of GPS data in pricing models have not been fully understood. Likewise, minimal research exists to evaluate the technical vulnerabilities that could be exploited to avoid criminal or financial penalties. To design a privacy-aware system, it is important to understand the needs of the stakeholders, most importantly the motorists. Knowledge about the anticipated privacy preferences of motorists is important in order to make reasonable predictions about their future willingness to adopt these systems. There is limited research so far on user perceptions regarding specific payment options in the uptake of privacy-aware systems.

This thesis provides a critical privacy assessment of two mobility pricing systems, namely electronic tolls and mobility-priced insurance. As a result of this assessment, policy recommendations are developed which could support a common approach in facilitating privacy-aware mobility-pricing strategies. This thesis also evaluates the existing and potential inferential threats and vulnerabilities to develop security and privacy recommendations for privacy-aware pricing designs for tolls and insurance. Utilising these policy recommendations and analysing user-perception with regards to the feasibility of sustaining privacy, and willingness to pay for privacy, two privacy-aware mobility pricing designs have been presented which bridge the entire array of privacy interests and bring them together into a unified approach capable of sustaining legal protection as well as satisfying privacy requirements of motorists. It is maintained that it is only by social and technical analysis working in tandem that critical privacy issues in relation to location can be addressed.

Declaration relating to disposition of project thesis/dissertation

I hereby grant to the University of New South Wales or its agents the right to archive and to make available my thesis or dissertation in whole or in part in the University libraries in all forms of media, now or here after known, subject to the provisions of the Copyright Act 1968. I retain all property rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstracts International (this is applicable to doctoral theses only).

Signature Witness Date

The University recognises that there may be exceptional circumstances requiring restrictions on copying or conditions on use. Requests for restriction for a period of up to 2 years must be made in writing. Requests for a longer period of restriction may be considered in exceptional circumstances and require the approval of the Dean of Graduate Research.

FOR OFFICE USE ONLY Date of completion of requirements for Award:

21/9/2009

THIS SHEET IS TO BE GLUED TO THE INSIDE FRONT COVER OF THE THESIS
LOCATION PRIVACY IN AUTOMOTIVE TELEMATICS

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Muhammad Usman Iqbal

School of Surveying & Spatial Information Systems, The University of New South Wales.

25 August 2009
ORIGINALITY STATEMENT

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project’s design and conception or in style, presentation and linguistic expression is acknowledged.

Signed

Date
COPYRIGHT STATEMENT

I hereby grant the University of New South Wales or its agents the right to archive and to make available my thesis or dissertation in whole or part in the University libraries in all forms of media, now or here after known, subject to the provisions of the Copyright Act 1968. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation. I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstract International (this is applicable to doctoral theses only). I have either used no substantial portions of copyright material in my thesis or I have obtained permission to use copyright material; where permission has not been granted I have applied/will apply for a partial restriction of the digital copy of my thesis or dissertation.

Signed

Date

AUTHENTICITY STATEMENT

I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis. No emendation of content has occurred and if there are any minor variations in formatting, they are the result of the conversion to digital format.

Signed

Date

1/09/09
PUBLICATIONS FROM THIS THESIS

The contributions claimed in this thesis has been published or under review in the following conferences/journals.

**Book Chapter(s):**


**Journal Paper(s):**


**Conference Papers:**


Media Coverage:


To my parents
Mr. Aftab Iqbal
& Mrs. Farhat Yasmin
without whose love and sacrifices
none of this would have been possible

in the loving memory of my Father-in-Law.
Mr. Zaki-uz-Zaman, whose kindness & support
would always remain with us as cherished thoughts.
Acknowledgments

I humbly thank Almighty Allah, Most Gracious, Most Merciful for giving me the health, the strength, the will and the curiosity to pursue this research. It is merely by the Grace of Allah that I have managed to complete this dissertation.

I have been indebted in the preparation of this thesis to my supervisor, Dr. Samsung Lim, whose patience and kindness, as well as his academic experience, have been invaluable to me. I am extremely grateful to Prof. Chris Rizos for his encouragement and invaluable advice. It was he whose lectures on location privacy back in 2003 sparked my interest in this field. I am also thankful to A/Prof. Andrew Dempster for his unwavering support of this work, and the exchange of ideas throughout the course of this research.

I would like to acknowledge the support of Ed Garvin, Managing Director of OMNILINK for having faith in my work, his encouragement and above all ensuring continuous funding throughout the course of this research. I also wish to thank all my colleagues at OMNILINK, the informal support and encouragement from them has been indispensable.

Special thanks to all staff at the School of Surveying whose friendship for their valuable company and constant encouragement. My sincere thanks to Sanaullah and Bilal for always being there when I needed their advice and support.

I would also like to thank my best friends Khurram, Omar, Kamran, Hamid, Dawar, Adnan, Ehsan, and oh yes, Moid for all the emotional support, comraderie, entertainment, and caring they provided.

I would like to extend my gratitude to OMNILINK and NUST for their financial support during this research.

I cannot end without thanking my family, on whose constant encouragement and love I have relied throughout my life. I thank my parents for the numerous sacrifices they made to get me to this stage. I would have been nowhere without their selfless love. I would also like to thank my brothers Murad, Faraz and Faran for their love and affection. I also thank my Grandmother, my mother-in-law, my aunts and uncles and my extended family for their prayers.

My daughter Zaynab and son Haani, the apples of my eyes, who bring joy and happiness to my life and soul. Lastly, and most importantly, to my affectionate wife Sana, who has been, always, my pillar, my joy and my guiding light, and I thank her.
Abstract

The convergence of transport, communication, computing and positioning technologies has enabled a smart car revolution. As a result, pricing of roads based on telematics technologies has gained significant attention. While there are promised benefits, systematic disclosure of precise location has the ability to impinge on privacy of a special kind, known as location privacy.

The aim of this thesis is to provide technical designs that enhance the location privacy of motorists without compromising the benefits of accurate pricing. However, this research looks beyond a solely technology-based solution. For example, the ethical implications of the use of GPS data in pricing models have not been fully understood. Likewise, minimal research exists to evaluate the technical vulnerabilities that could be exploited to avoid criminal or financial penalties. To design a privacy-aware system, it is important to understand the needs of the stakeholders, most importantly the motorists. Knowledge about the anticipated privacy preferences of motorists is important in order to make reasonable predictions about their future willingness to adopt these systems. There is limited research so far on user perceptions regarding specific payment options in the uptake of privacy-aware systems.

This thesis provides a critical privacy assessment of two mobility pricing systems, namely electronic tolls and mobility-priced insurance. As a result of this assessment, policy recommendations are developed which could support a common approach in facilitating privacy-aware mobility-pricing strategies. This thesis also evaluates the existing and potential inferential threats and vulnerabilities to develop security and privacy recommendations for privacy-aware pricing designs for tolls and insurance. Utilising these policy recommendations and analysing user-perception with regards to the feasibility of sustaining privacy, and willingness to pay for privacy, two privacy-aware mobility pricing designs have been presented which bridge the entire array of privacy interests and bring them together into a unified approach capable of sustaining legal protection as well as satisfying privacy requirements of motorists. It is maintained that it is only by social and technical analysis working in tandem that critical privacy issues in relation to location can be addressed.
# Contents

### List of Acronyms  
xxiv

## 1 Introduction  
1. The Union of Space & Time on Roads  
2. Research Motivation  
3. Research Aims  
4. Thesis Outline  
5. Contribution  

## 2 Telematics Concepts  
2.1 Introduction  
2.2 Telematics  
2.2.1 Definition  
2.2.2 Automotive Telematics  
2.2.3 Intelligent Transportation Systems (ITS)  
2.2.4 Relationship between Telematics and ITS  
2.3 Building Blocks of Telematics  
2.3.1 Positioning Techniques  
2.3.2 Communications  
2.3.3 Computing  
2.3.4 Geospatial Data Management  
2.4 Commercial Telematics Systems  
2.5 Mobility Pricing  
2.5.1 Electronic Toll Collection (ETC)  
2.5.2 Mobility Priced Insurance  
2.6 Summary  

## 3 Location Privacy Concepts  
3.1 Introduction  
3.2 Privacy Concepts  
3.2.1 History of Privacy  
3.2.2 Privacy in the Modern World  
3.2.3 Various Facets of Privacy  

xv
CONTENTS

3.3 Important Concepts Related to Privacy ........................................ 49
  3.3.1 Surveillance .......................................................... 49
  3.3.2 Dataveillance ......................................................... 51
  3.3.3 Uberveillance ......................................................... 52
  3.3.4 Tracking ............................................................. 52
  3.3.5 Anonymity ........................................................... 53
  3.3.6 Identity ............................................................. 54

3.4 Location Privacy .......................................................... 54
  3.4.1 Definition .......................................................... 55
  3.4.2 Location Privacy Classification .................................... 55
  3.4.3 Telematics & Privacy ................................................. 57

3.5 Social Mechanisms for Privacy Protection ................................... 60
  3.5.1 Ethics ............................................................... 60
  3.5.2 Trust ................................................................. 61
  3.5.3 Societal Norms ..................................................... 62
  3.5.4 Social Survey Research ............................................ 64

3.6 Legal Mechanisms for Privacy Protection .................................... 65
  3.6.1 Legislative Frameworks ............................................. 66
  3.6.2 Case Law .......................................................... 70

3.7 Technical Mechanisms for Privacy Protection ............................... 73
  3.7.1 Policy-based & Rule-based protections ............................ 73
  3.7.2 Decoupling Identity & Location .................................. 74
  3.7.3 Anonymous Access ................................................ 74
  3.7.4 Obfuscation ....................................................... 75
  3.7.5 Privacy-aware designs ............................................. 76

3.8 Research Gap: Privacy-aware Mobility Pricing ............................... 76

3.9 Summary ................................................................. 78

4 Privacy Assessment of Two Mobility-Priced Applications ................. 79
  4.1 Introduction .......................................................... 79
  4.2 Analysis Framework .................................................. 80
    4.2.1 Non-Electronic Equivalence Test ................................. 80
    4.2.2 Active vs. Passive Systems .................................... 80
    4.2.3 Identifiability .................................................. 81
    4.2.4 Consent and Choice ............................................. 82
    4.2.5 Locational Granularity ........................................ 82
  4.3 Case Study I: Electronic Toll Collection ................................ 82
    4.3.1 Privacy Implications of Existing Tolling Practices .......... 82
    4.3.2 Unique Identifiers ............................................. 85
    4.3.3 Extended Data Retention ...................................... 85
    4.3.4 Secondary uses ................................................ 87
    4.3.5 Security Vulnerabilities ....................................... 89
    4.3.6 Legislative Instruments ....................................... 90
### CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.7 Standard for Privacy of Toll Collection</td>
<td>90</td>
</tr>
<tr>
<td>4.3.8 Disregard of NPP and Privacy Standard</td>
<td>91</td>
</tr>
<tr>
<td>4.3.9 Review of Toll Applications</td>
<td>92</td>
</tr>
<tr>
<td>4.3.10 Survey Research</td>
<td>95</td>
</tr>
<tr>
<td>4.3.11 Analysis Framework</td>
<td>96</td>
</tr>
<tr>
<td>4.3.12 Policy Recommendations</td>
<td>100</td>
</tr>
<tr>
<td>4.4 Case Study II: Mobility-Priced Insurance</td>
<td>103</td>
</tr>
<tr>
<td>4.4.1 Privacy Issues in Various Mobility-Priced Options</td>
<td>103</td>
</tr>
<tr>
<td>4.4.2 Towards Legislation for Pay-as-you-drive (PAYD)</td>
<td>105</td>
</tr>
<tr>
<td>4.4.3 Secondary uses</td>
<td>106</td>
</tr>
<tr>
<td>4.4.4 Analysis Framework</td>
<td>107</td>
</tr>
<tr>
<td>4.4.5 Policy Recommendations</td>
<td>109</td>
</tr>
<tr>
<td>4.5 Summary</td>
<td>111</td>
</tr>
<tr>
<td>5 Analysis of Threats &amp; Vulnerabilities of GPS Data</td>
<td>113</td>
</tr>
<tr>
<td>5.1 Introduction</td>
<td>113</td>
</tr>
<tr>
<td>5.2 Inferential Threats From Automated Profiling</td>
<td>114</td>
</tr>
<tr>
<td>5.2.1 Inference Attack</td>
<td>115</td>
</tr>
<tr>
<td>5.2.2 Threat Model</td>
<td>116</td>
</tr>
<tr>
<td>5.2.3 Apparatus</td>
<td>116</td>
</tr>
<tr>
<td>5.2.4 Passive Surveillance</td>
<td>117</td>
</tr>
<tr>
<td>5.2.5 Interception and Analysis</td>
<td>118</td>
</tr>
<tr>
<td>5.2.6 Profile Generation</td>
<td>122</td>
</tr>
<tr>
<td>5.2.7 Evaluation</td>
<td>128</td>
</tr>
<tr>
<td>5.2.8 Recommendation</td>
<td>129</td>
</tr>
<tr>
<td>5.3 Legal &amp; Ethical Implications of GPS Vulnerabilities</td>
<td>131</td>
</tr>
<tr>
<td>5.3.1 Legal Scenarios</td>
<td>131</td>
</tr>
<tr>
<td>5.3.2 Commercial Scenarios</td>
<td>135</td>
</tr>
<tr>
<td>5.3.3 Vulnerability Assessment</td>
<td>135</td>
</tr>
<tr>
<td>5.3.4 Threat Model</td>
<td>137</td>
</tr>
<tr>
<td>5.3.5 Apparatus</td>
<td>137</td>
</tr>
<tr>
<td>5.3.6 Malicious Editing</td>
<td>138</td>
</tr>
<tr>
<td>5.3.7 Spoofing Attack</td>
<td>142</td>
</tr>
<tr>
<td>5.3.8 Evaluation</td>
<td>144</td>
</tr>
<tr>
<td>5.3.9 Countermeasures</td>
<td>145</td>
</tr>
<tr>
<td>5.3.10 Recommendation</td>
<td>147</td>
</tr>
<tr>
<td>5.4 Summary</td>
<td>148</td>
</tr>
<tr>
<td>6 Methodological Assessment of User Perspective of Telematics</td>
<td>149</td>
</tr>
<tr>
<td>6.1 Introduction</td>
<td>149</td>
</tr>
<tr>
<td>6.2 A Preliminary Survey of Online Attitudes</td>
<td>151</td>
</tr>
<tr>
<td>6.2.1 Instrumentation</td>
<td>151</td>
</tr>
<tr>
<td>6.2.2 Video Clip</td>
<td>151</td>
</tr>
</tbody>
</table>
6.2.3 Questionnaire ........................................... 152
6.2.4 Sample Space ........................................... 153
6.2.5 Key Findings ........................................... 154
6.2.6 Conclusion ............................................. 158
6.3 A Detailed Assessment of Location Experts ......... 158
6.3.1 Instrumentation ........................................ 159
6.3.2 Sample Space ........................................... 160
6.3.3 Data Collection ........................................ 162
6.3.4 Analysis ................................................. 163
6.4 Principal Findings for Telematics .................... 165
6.4.1 Respondents' Awareness/Interest in Telematics ... 165
6.4.2 Perceived Threat of Telematics Technologies .... 165
6.4.3 Privacy Remedies ...................................... 166
6.5 Principal Findings for ETC ............................ 167
6.5.1 Awareness of and Concerns about Tolling ....... 167
6.5.2 Inclination Towards Post-Paid Anonymity .......... 170
6.5.3 Demographics and Payment Choices ............... 172
6.6 Principal Findings for GPS-Enabled Insurance ...... 174
6.6.1 Privacy-Aware Insurance Scenarios ................. 174
6.6.2 Correlation of Privacy Choices and Demographics 177
6.6.3 Qualitative Analysis .................................. 180
6.7 Summary ................................................. 182
7 User-Perception Inspired Privacy-Aware Models ....... 185
7.1 Introduction .............................................. 185
7.2 Privacy-Aware GPS-Enabled Insurance ............... 186
7.2.1 Results for Insurance from the Analytical Framework 186
7.2.2 Results on GPS-based Insurance from the Threat Model 187
7.2.3 Survey Results on Privacy-aware Insurance ....... 187
7.2.4 Conceptual Design ................................... 188
7.2.5 Description .......................................... 191
7.2.6 System Evaluation .................................... 203
7.2.7 Conclusion .......................................... 207
7.3 Post-Paid Anonymous Toll Collection ............... 208
7.3.1 Results on ETC from the Privacy Analytical Framework 208
7.3.2 Survey Results on ETC ............................... 209
7.3.3 Protocol Requirements .............................. 210
7.3.4 Cryptographic Building Blocks .................... 211
7.3.5 Conceptual Design .................................. 212
7.3.6 Protocol Details .................................... 217
7.3.7 Other Implementation Options .................... 220
7.3.8 Conclusion .......................................... 221
7.4 Infrastructureless Tolls and Insurance .............. 222
CONTENTS

8 Conclusion
  8.1 Summary of Results 225
  8.2 Thesis Limitations 228
  8.3 Future Work 229

A Survey Questionnaire: Preliminary Online Survey 231

B IGNSS Conference Survey 237
List of Tables

2.1 Summary of electronic tolling operations in Australia. . . . . . . . 33
3.1 ITS technologies with potential privacy concerns. . . . . . . . . . 59
3.2 Summary of National Privacy Principles (NPP)s. . . . . . . . . . 68
4.1 Toll Roads and Number of Toll Gantry in Sydney. . . . . . . . . 99
4.2 Summary of the analysis framework results for ETC. . . . . . . . 101
4.3 Comparison of insurance approaches for cost, privacy and accuracy. 104
4.4 Summary of the analysis framework results for PAYD insurance. . 110
5.1 Protocol output of inferred home location compared with actual street address obtained from post-exercise interview. . . . . . . . 122
5.2 Profile Summary of volunteers generated by the software protocol. 125
6.1 Demographic profile of respondents (N=78). . . . . . . . . . 162
6.2 Respondents ranking of technologies for privacy-invasiveness . . 165
6.3 Respondents’ ranking of privacy solutions in terms of effectiveness 168
6.4 Awareness of fully electronic tolling decision in NSW . . . . . . 169
6.5 Perceived threats to privacy . . . . . . . . . . . . . . . . . . . . . . 169
6.6 Perceived interest in an anonymous cashless tolling system . . 171
6.7 Distribution of amount pledged for three design alternatives. . . 176
6.8 Respondents reason for disinterest in the 3 design choices. . . . 181
7.1 A possible catalogue of weather conditions & associated risk. . . 194
7.2 A possible catalogue of visibility conditions & associated risk. . 195
List of Figures

2.1 Possible telematics-driven services. ........................................ 9
2.2 Critical components of telematics. ........................................ 11
2.3 Monograms of noteworthy GNSS systems. Sources (Galileo 2007; GLONASS 2008; GPS 2008) ........................................ 15
2.4 Message exchange between telematics provider and subscribed vehicle. ........................................ 19
2.5 An electronic toll tag. ........................................ 20
2.6 Telematics in operation. ........................................ 25
2.7 An illustration of commercial telematics systems. ........................................ 26
2.8 A conceptual user interface for electronic parking. Source (Parking Angel, 2008) ........................................ 28
2.9 How electronic toll collection systems work. ........................................ 31
2.10 Example of how a distance-based toll is calculated. Source (West-Link M7, 2008) ........................................ 34
2.11 How GPS-based insurance works. Source (Norwich Union, 2007) ........................................ 37
2.12 A sample bill of charges for Norwich Union’s PAYD, Source (Norwich Union, 2007) ........................................ 40

3.1 An illustration of the types of location information in the proposed classification. ........................................ 57

4.1 An illustration of registration and transactional data collection for ETC. ........................................ 84
4.2 The Houston Transtar application visualises current traffic conditions on a map. Source (Houston Transtar, 2008) ........................................ 88
4.3 Mcloak pouch used for shielding toll tag signals. Source (Mobile Cloak, 2009) ........................................ 89

5.1 A typical adversarial threat model. ........................................ 116
5.2 Details of the Global Positioning System (GPS) device used. ........................................ 117
5.3 GPS track data downloaded onto PC from GPS device. ........................................ 118
5.4 GNAF data model. Source: (GNAF Product Description, 2009) ........................................ 120
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5</td>
<td>Street address of volunteer ‘J’ incorrectly guessed by home determination algorithm.</td>
</tr>
<tr>
<td>5.6</td>
<td>A snapshot of whitepages.com.au’s residential address form.</td>
</tr>
<tr>
<td>5.7</td>
<td>Speed and Acceleration graphs for Volunteer ‘J’.</td>
</tr>
<tr>
<td>5.8</td>
<td>GPS track data downloaded onto PC from GPS device.</td>
</tr>
<tr>
<td>5.9</td>
<td>A taxonomy of possible interference sources to GPS signals.</td>
</tr>
<tr>
<td>5.10</td>
<td>Threat model used in this experiment.</td>
</tr>
<tr>
<td>5.11</td>
<td>The range of GPS devices used for the experiments.</td>
</tr>
<tr>
<td>5.12</td>
<td>Editing route shown on a spatial map.</td>
</tr>
<tr>
<td>5.13</td>
<td>The GPS receivers removed from their casings.</td>
</tr>
<tr>
<td>5.14</td>
<td>A schematic representation of GPS hardware illustrating spoof and authentic signals at receiver antenna.</td>
</tr>
<tr>
<td>5.15</td>
<td>The Spirent 6560 Signal Generator used.</td>
</tr>
<tr>
<td>5.16</td>
<td>The re-radiator antenna used for broadcasting fake GPS signals.</td>
</tr>
<tr>
<td>6.1</td>
<td>Some scenes from the animation that respondents watched before taking the preliminary survey.</td>
</tr>
<tr>
<td>6.2</td>
<td>Bar-chart depicting respondent choices of new privacy-preserving insurances.</td>
</tr>
<tr>
<td>6.3</td>
<td>Bar-chart representing correlation between rewards-program subscription and gender.</td>
</tr>
<tr>
<td>6.4</td>
<td>Distribution of respondents’ profession.</td>
</tr>
<tr>
<td>6.5</td>
<td>Boxplot representing distribution of interest in telematics and GPS.</td>
</tr>
<tr>
<td>6.6</td>
<td>Boxplot representing distribution of perceived threats of telematics and secondary uses of data.</td>
</tr>
<tr>
<td>6.7</td>
<td>Respondents’ perceived threat of tracking and secondary uses of toll data.</td>
</tr>
<tr>
<td>6.8</td>
<td>Distribution of interest in anonymous and cashless accounts.</td>
</tr>
<tr>
<td>6.9</td>
<td>Respondents preferred anonymous payment option.</td>
</tr>
<tr>
<td>6.10</td>
<td>Respondents’ opinion on pre-pay vs. post-pay anonymity.</td>
</tr>
<tr>
<td>6.11</td>
<td>Box-plot showing relationship amongst payment type, gender and interest in anonymity.</td>
</tr>
<tr>
<td>6.12</td>
<td>Boxplot showing relationship amongst age, payment type and interest in anonymity.</td>
</tr>
<tr>
<td>6.13</td>
<td>Boxplot representing distribution of amount willing to be pledged for the 3 types of mobility-priced insurance scenarios.</td>
</tr>
<tr>
<td>6.14</td>
<td>Boxplot representing correlation between respondent’s vehicle type and distribution of interest for the 3 types of mobility-priced insurance scenarios.</td>
</tr>
<tr>
<td>6.15</td>
<td>Boxplot representing correlation between respondents’ gender and distribution of interest for the 3 types of mobility-priced insurance scenarios.</td>
</tr>
</tbody>
</table>
6.16 Boxplot representing correlation between respondents’ age and distribution of interest for the 3 types of mobility-priced insurance scenarios. ............................................. 180
7.1 The difference between existing and proposed designs. .......... 190
7.2 Schematic representation of the Privacy-aware GPS-enabled insurance model. ............................. 192
7.3 A snapshot of the user-interface. ................................................. 199
7.4 Dispute Resolution Protocol. ...................................................... 202
7.5 Steps involved in registration, toll event and toll collection. .... 213
7.6 Spatio-temporal details of trip stored in motorist’s transponder. . 215
7.7 An illustration of the entities and stages of the protocol. .......... 216
7.8 Sequence of message exchange in a closed tolling system. ........ 219
List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAP</td>
<td>Active Accelerator Pedal</td>
</tr>
<tr>
<td>ACMA</td>
<td>Australian Communications and Media Authority</td>
</tr>
<tr>
<td>ABS</td>
<td>Australian Bureau of Statistics</td>
</tr>
<tr>
<td>AFS</td>
<td>Advanced Front-lighting System</td>
</tr>
<tr>
<td>AGPS</td>
<td>Assisted-GPS</td>
</tr>
<tr>
<td>ALRC</td>
<td>Australian Law Reform Commission</td>
</tr>
<tr>
<td>ANPR</td>
<td>Automatic Number Plate Recognition</td>
</tr>
<tr>
<td>AOA</td>
<td>Angle of Arrival</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AUD</td>
<td>Australian Dollar</td>
</tr>
<tr>
<td>AVI</td>
<td>Advance Vehicle Identification</td>
</tr>
<tr>
<td>C/A</td>
<td>Course/Acquisition</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit Television</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical infrastructure protection</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-separated values</td>
</tr>
<tr>
<td>DoT</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communications</td>
</tr>
<tr>
<td>E911</td>
<td>Enhanced 911</td>
</tr>
</tbody>
</table>
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETC</td>
<td>Electronic Toll Collection</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ETR</td>
<td>Express Toll Route</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Consortium</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographical Information System</td>
</tr>
<tr>
<td>GLONASS</td>
<td>GLObal'naya NAvigatsionnaya Sputnikovaya Sistema</td>
</tr>
<tr>
<td>GM</td>
<td>General Motors</td>
</tr>
<tr>
<td>GNAF</td>
<td>Geo-coded National Address File</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPX</td>
<td>GPS eXchange Format</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IFF</td>
<td>Identification, friend or foe</td>
</tr>
<tr>
<td>IPC</td>
<td>Information and Privacy Commissioner</td>
</tr>
<tr>
<td>IPP</td>
<td>Information Privacy Principles</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation Systems</td>
</tr>
<tr>
<td>IOS</td>
<td>Insurance Ombudsman Service</td>
</tr>
<tr>
<td>IRNSS</td>
<td>Indian Regional Navigational Satellite System</td>
</tr>
<tr>
<td>ISA</td>
<td>Intelligent Speed Adaptation</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>KML</td>
<td>Keyhole Markup Language</td>
</tr>
<tr>
<td>LBS</td>
<td>Location Based Services</td>
</tr>
<tr>
<td>LCR</td>
<td>Light Conditions Risk</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agencies</td>
</tr>
<tr>
<td>LGA</td>
<td>Local Government Area</td>
</tr>
<tr>
<td>MB</td>
<td>Megabytes</td>
</tr>
<tr>
<td>MRF</td>
<td>Mileage Rate Factor</td>
</tr>
<tr>
<td>NMEA</td>
<td>National Marine Electronics Association</td>
</tr>
<tr>
<td>NNSS</td>
<td>Navy Navigational Satellite System</td>
</tr>
<tr>
<td>NPP</td>
<td>National Privacy Principles</td>
</tr>
<tr>
<td>NRMA</td>
<td>National Roads and Motorists Association</td>
</tr>
<tr>
<td>NSW</td>
<td>New South Wales</td>
</tr>
<tr>
<td>OBE</td>
<td>On-board equipment</td>
</tr>
<tr>
<td>OBD-II</td>
<td>On-board diagnostics port</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>P3P</td>
<td>Platform for Privacy Preferences</td>
</tr>
<tr>
<td>P-Code</td>
<td>Precision Code</td>
</tr>
<tr>
<td>PATP</td>
<td>Pay-at-the-pump</td>
</tr>
<tr>
<td>PAYD</td>
<td>Pay-as-you-drive</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>Personal Computer Memory Card International Association</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PDAs</td>
<td>Personal Digital Assistants</td>
</tr>
<tr>
<td>PNI</td>
<td>Primary Named Insured</td>
</tr>
<tr>
<td>POIs</td>
<td>Points of interest</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PIPP</td>
<td>Personal Information Protection Principles</td>
</tr>
<tr>
<td>PPIP</td>
<td>Privacy and Personal Information Protection Act 1998 (NSW)</td>
</tr>
<tr>
<td>PPS</td>
<td>Precise Positioning Service</td>
</tr>
<tr>
<td>PRN</td>
<td>Pseudo Range Number</td>
</tr>
<tr>
<td>PSMA</td>
<td>Public Sector Mapping Agencies</td>
</tr>
<tr>
<td>PVT</td>
<td>position, velocity and time</td>
</tr>
<tr>
<td>QZSS</td>
<td>Quasi-Zenith Satellite System</td>
</tr>
<tr>
<td>RDS-TMC</td>
<td>Radio Data System Travel Message Channel</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RHR</td>
<td>Rush Hour Risk</td>
</tr>
<tr>
<td>RR</td>
<td>Road Risk</td>
</tr>
<tr>
<td>RSE</td>
<td>Road Side Equipment</td>
</tr>
<tr>
<td>RSS</td>
<td>Received signal strength</td>
</tr>
<tr>
<td>RSW</td>
<td>Rain-sensing wipers</td>
</tr>
<tr>
<td>RACV</td>
<td>Royal Automobile Club of Victoria</td>
</tr>
<tr>
<td>SATNAV</td>
<td>Satellite Navigation</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SPS</td>
<td>Standard Positioning Service</td>
</tr>
<tr>
<td>SPSS</td>
<td>Statistical Package for the Social Sciences</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SR</td>
<td>Speeding Risk</td>
</tr>
<tr>
<td>TISA</td>
<td>Traveller Information Services Association</td>
</tr>
<tr>
<td>TOA</td>
<td>Time of Arrival</td>
</tr>
<tr>
<td>TDOA</td>
<td>Time Difference of Arrival</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra Wide-band</td>
</tr>
<tr>
<td>VANET</td>
<td>Vehicular Ad-hoc Networks</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>WCR</td>
<td>Weather Conditions Risk</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 The Union of Space & Time on Roads

In recent years, the pace with which technology develops continues to challenge human belief. From the first attempts on farming in the Fertile Crescent in 5 Millennium BC to the invention of the first wheel, lies a period of four thousand years. The inventions of the automobile, computers, the database, internet, GPS-satellites and both wired and wireless telecommunication all took place in the last century.

These technologies continue to revolutionise the way people interact with each other and machines, and offer many benefits to humanity. Yet, at the same time, these technologies continue to erode personal privacy. It was a technical innovation, the camera, that first created the phrase, 'the right to privacy' in 1890 (Warren & Brandeis, 1890).

The convergence of positioning, communication and computing technologies in the automotive arena has enabled a smart car revolution, where both cars and roads have become sophisticated. Within the realm of this smart car revolution, mobility pricing has gained recent attention, where different taxes, levies and insurance premium can be priced on the basis of actual mileage, and provide a
fairer reflection of cost vs. usage than previously.

While there are apparent benefits in using telematics-driven payment systems, the convergence of these technologies has begun to challenge the anonymity that motorists have so far enjoyed. These systems have the potential to enable systematic mass surveillance and to impinge on privacy of a special kind, known as location privacy. Current payment mechanisms require the location and tracking of people to identify them and charge them accurately, by either actively identifying them on a particular tolled road or reactively collating their travel routes for the underwriting of mileage-based insurance policies. It seems that a new era of reterritorialisation has begun where systematic monitoring of time and place have become relevant (Nouwt, 2008). The new frontier for privacy is not in cyberspace anymore, but in public-spaces which are highly connected and highly mobile.

1.2 Research Motivation

The pace at which location and communication technologies are converging is extremely rapid. The potential impacts of these technologies on society are also highly significant. These developments warrant a closer scrutiny of any future technologies that may disrupt the balance and harmony between technology and society. The pricing of roads is inevitable, and will be implemented to tackle congestion on roads, to reduce negative environmental effects and to provide fair taxes and levies.

Privacy is a social issue, but it is making headlines because of technological impacts. It is important for those with technical training to pay close attention to social issues surrounding technologies. An understanding of the technical details is essential to evaluate the social, legal and ethical issues that arise from technological advancements. Therefore, technologists have a social responsibility to utilise their expertise in order to assist in the evaluation of related social
1. Introduction

issues. It is only by combining social and technical analysis that problems will be resolved. This thesis is an engineer’s attempt at examining the privacy issues of mobility-pricing as seen today and at proposing privacy-aware designs which address the needs of all stakeholders.

1.3 Research Aims

The principal aim of this thesis is to investigate and develop privacy-aware mobility-pricing designs. This broad aim may be expressed in terms of a number of objectives:

- To review literature in the fields of telematics and location privacy to identify where these two intersect, and what are the potential causes of concern with regards to location privacy and mobility-pricing.

- To review the legal framework for support of location privacy and evaluate the lack thereof.

- To analyse issues prompting decline of past anonymous road-pricing options.

- To stimulate thinking and research about neglected approaches to privacy-preservation that are outside typical technology practices.

- To analyse the potential privacy implications of electronic pricing applications via case-study-based research.

- To examine the potential barriers that have to be crossed in terms of technology and social aspects to restore anonymity of travel on roads.

- To evaluate the implications of the collection, retention and processing of precise location information and the threats possible from inferencing and data-mining.
1. Introduction

- To analyse the difference between private information and location information. What characteristics of location information make it unique or potentially more invasive than other information allowing personal identification?

- To analyse technology vulnerabilities of positioning systems that have legal and commercial implications.

- To study user-perception of pricing and privacy options for mobility-pricing.

- To design privacy-preserving toll collection systems that restore anonymity on roads.

- To design mobility-priced insurance systems that offer fair premiums and accurate reflection of risks without compromising privacy.

1.4 Thesis Outline

This thesis comprises 8 chapters each of which addresses a specific piece of the overall problem of mobility-pricing and location privacy. Chapter 1 has briefly introduced the problem space, the motivation to conduct this research, the research objectives and the potential contributions of this thesis.

Chapter 2 presents a review of telematics technologies and provides details of the essential building blocks of telematics. It also describes how these technologies have enabled road-pricing.

Chapter 3 provides a brief review of etymological and legal history of privacy. The chapter also introduces location privacy and examines current protection mechanisms from legal, social and technical contexts.
1. Introduction

Chapter 4 supplements Chapter 3 by critically analysing the privacy challenges faced in two distinct yet related pricing applications, electronic tolls and PAYD. These challenges are then evaluated by an analytical framework which compares the two applications on a select criteria and provides a privacy assessment of these two applications. It then makes policy recommendations useful for development of privacy strategies.

Chapter 5 performs a technology analysis of the inferential threats possible by using GPS data and the vulnerabilities that may be exploited to avoid criminal or financial penalties in an effort to highlight that the impacts of the use of precise location information may be well beyond current realisation, and to note the importance of curtailing access to this data.

Chapter 6 examines user perception and attitudes to privacy-aware mobility-pricing. It demonstrates the relationship between the decline of anonymous payment options and the difficulties in pursuing those options. It also deals with the questions of the feasibility of maintaining privacy and of the willingness to pay for privacy.

Chapter 7 combines the results obtained from Chapters 4, 5, & 6 into a coherent whole and constructs nuanced privacy-aware technological designs which bridge the entire array of privacy interests and bring them together into a unified approach capable of sustaining legal protection as well as satisfying privacy requirements of motorists.

Chapter 8 highlights the achievements of this work and suggests topics for future research.
1.5 Contribution

The major contributions of this research can be summarised as follows:

- A privacy assessment of the invasiveness of electronic tolls and GPS-enabled insurance, in terms of choice, consent, spatial granularity, identifiability and non-electronic equivalent has been presented (Chapter 4).

- Policy recommendations that could support a common approach to facilitating the development of strategies for privacy-aware mobility-pricing have been made (Chapter 4).

- A critical analysis of the inferential threats from precise GPS data has been performed and proposals to minimise disclosure of this data due to potential sensitivities has been proposed (Chapter 5).

- The technological vulnerabilities that could be exploited for gaining financial benefits or evading legal proceedings have been evaluated and recommendations are made to minimise these security gaps (Chapter 5).

- User-perception regarding privacy-aware payment systems and privacy options have been assessed. Results of this survey have served to extend understanding of user perspectives in the design of privacy-aware systems (Chapter 6).

- A post-paid anonymous toll collection system which preserves motorists' privacy and offers the choice of paying later has been presented (Chapter 7).

- A pay-how-you-drive system which accurately reflects road risks and preserves privacy of motorists has been devised (Chapter 7).

- Mechanisms developed that provide the ability to verify that payment is being accurately charged (Chapter 7).
Chapter 2

Telematics Concepts

2.1 Introduction

This chapter provides a background to how the availability of precise location information is creating novel opportunities for car manufacturers, transport planners, insurance providers and motorists. This chapter presents a review of the relevant literature in the field of telematics. The development of telematics is addressed in Section 2.2, providing a brief account from historical perspectives, of how the telematics of today evolved. This is followed by a discussion of the building blocks of telematics in Section 2.3, involving the converging evolution of telecommunications, positioning, computing and cartography, which has revolutionised context-aware automotive applications. Commercial applications of automotive telematics being developed by car manufacturers are reviewed in Section 2.4. Finally, in Section 2.5, this chapter focuses on how these technologies have enabled mobility-pricing of roads. An overview of pricing of roads is provided with an in-depth analysis of two distance-based pricing technologies. One of these technologies, ETC, was introduced almost two decades ago, while the other one, mobility-priced insurance, is slowly growing.
2.2 Telematics

2.2.1 Definition

There are two possible definitions for the word ‘telematics’. The first relates to the French word ‘Télématique’, which was originally coined to mean the convergence of telecommunications and information processing (informatique in French) (Nora & Minc, 1980).

The second etymological definition of telematics, is the product of two Greek words, ‘tele’ (meaning ‘far away’), and matos (meaning ‘of its own accord’), which, when combined in the term telematics, describes the process of long-distance transmission of computer-based information (Foy, 2002).

Telematics is the blending of computers and wireless telecommunications technologies, with the perceived goal of efficiently conveying information over vast networks. The most obvious example of telematics is the Internet, which depends on a number of computer networks connected globally through telecommunications backbones.

2.2.2 Automotive Telematics

The term has gradually evolved from a general meaning to an automotive industry expression and is generally used for Automotive Telematics. Automotive Telematics combines communications, positioning and computing technologies on-board a vehicle to improve the safety, security and comfort of vehicle occupants (Foy, 2002).

Satellite navigation is becoming increasingly available on new mid-range car models as a standard feature. Likewise, after-market GPS products are also becoming increasingly affordable and available. This capability permits the use of positioning equipment for other value added services.

Researchers have started exploring opportunities of offering novel applica-
2. Telematics Concepts

Figure 2.1: Possible telematics-driven services.

Tions in the automotive sector by using positioning technologies. A range of services, as shown in Figure 2.1, is being planned or implemented, such as in-car navigation, roadside assistance, infotainment, satellite-tracking of lost/stolen vehicles, vehicular internet access, traffic monitoring, custom weather reports, parental vehicle tracking, emergency response services, remote diagnostics and prognostics, asset monitoring, fleet management, road-pricing and vehicle insurance (Grush, 2005; Zhang, Wang, & Hackbarth, 2003; Vidales & Stajano, 2002; Vrhovski, Moore, & Bennett, 2004; Enkelmann, 2003; Campos, Mills, & Graves, 2002).
2.2.3 Intelligent Transportation Systems (ITS)

ITS is an international initiative to apply information and communications technology to transport infrastructures and automobiles in order to improve road safety and fuel consumption and therefore reduce transportation time (Whelan, 1995). In Australian contexts, ITS has been defined as,

"The application of modern computer and communication technologies to transport systems, to increase efficiency, reduce pollution and other environmental effects of transport and to increase the safety of the travelling public." (ITS Australia, 1998)

Interest in ITS comes from the problems caused by traffic congestion and the synergy of new information technology. Traffic congestion has been increasing worldwide as a result of increased motorization, urbanization, population growth, and changes in population density. Congestion reduces efficiency of transportation infrastructure and increases travel time, air pollution, and fuel consumption. In general ITS applications there is no need to identify a particular vehicle since the aggregate information is sufficient to perform ITS services. However, recent developments in transport technology, with the agenda of enforcement, policing, road safety, national security and road pricing, are systematically requiring the road-users' identity, either with the help of contracts such as ETC systems, or through visual interfaces such as Automatic Number Plate Recognition (ANPR) which extracts the licence plate details from a photo electronically.

2.2.4 Relationship between Telematics and ITS

The development of ITS has been underway for several years now. During this time, there have been dramatic changes in telecommunications and computing technologies, especially in mobile communications and computing. The cost of secondary storage has also remarkably decreased, enabling vast amounts of data
processing and storage. This unprecedented technical growth in vehicle-based systems has become part of the classical ITS, and is commonly known as telematics. Thus telematics is an enabler of the ITS vision, and plays a supportive role in integrating vehicles with advanced communications and information technologies to move people and goods more safely, efficiently, and comfortably.

2.3 Building Blocks of Telematics

Telematics combines positioning, communication and computing to create automated services that are environmentally intelligent, as illustrated in Figure 2.2. The following sections look at each of these building blocks in detail.

2.3.1 Positioning Techniques

'Geo-positioning' or 'position determination' is a crucial technology for telematics. Before moving on to how positioning is done, it is necessary to establish
2. Telematics Concepts

a definition of what constitutes location. Clarke (1999b) defines location as follows.

"By an entity's location is meant a description of its whereabouts, in relation to other, known objects or reference points."

A telematics application should be able to determine an entity's current location or position with respect to a reference frame, in order to answer simple queries like 'where am I?', to more complex ones like 'how to route from a point X to a point Y against certain criteria?' (Raper, Gartner, Karimi, & Rizos, 2007).

Satellite Navigation Techniques

The first satellite navigation system, the Navy Navigational Satellite System (NNSS), also known as TRANSIT, was a system deployed by the US military in the 1960s. It consisted of six satellites and was primarily used by naval vessels and aircraft to determine their coordinates. It was a military owned and operated system, but later civilian use was also authorised. TRANSIT's operation was based on the Doppler effect, where the received frequency differs slightly from the broadcast frequency because of the movement of the satellite with respect to the receiver. The measurements of Doppler shift combined with a precise knowledge of the satellite's orbit gave a positional fix (Parkinson, Stansell, Beard, & Gromov, 1995). Transit was phased out in 1997.

Modern satellite systems are different. The satellite broadcasts a signal that contains the position of the satellite and the precise time the signal was transmitted. All satellites in the constellation are synchronized by using atomic clocks. The receiver compares the transmission time with reception time, measured by an internal clock, thereby measuring the time-of-flight of the satellite's signal. Each distance measurement places the receiver on a spherical shell at the measured distance from the satellite. By taking several such measurements and then
looking for a point where these spheres intersect, a position fix is generated (Tsui, 2000).

The best known satellite positioning and navigation system is the NAVSTAR GPS. GPS is a satellite-based radio-positioning and time-transfer system developed by the United States (US) Department of Defence to support real-time navigation anywhere on the earth (Parkinson & Spilker, 1996). The system has the advantage of being globally accessible, functioning independently of local weather conditions, and being able to provide three-dimensional position, velocity and time (PVT) in a common reference system, anywhere on or near the surface of the earth, on a continuous basis. GPS, in the same way as TRANSIT, was developed for military purposes, but eventually civilians were allowed to use it.

The GPS system comprises three segments. The Space Segment nominally comprises 24 satellites (with 3 spares), in six circular orbital planes at an altitude of about 20,200 km above the earth’s surface, with an orbital inclination of 55 degrees. The exact number of satellites varies as satellites are replenished when older ones are retired. The constellation design is such that at least four satellites are simultaneously visible above the horizon anywhere on the earth, 24 hours a day. The Control Segment consists of the ground facilities carrying out the task of satellite tracking, orbit computations, telemetry and supervision necessary for the continuous operation of the Space Segment. There are five primary ground facility stations located around the world. The User Segment refers to the many positioning and navigation applications available to both military and civilian users (Rizos, 2005).

GPS services vary, depending on the identity of the user. The two service modes that exist are Precise Positioning Service (PPS), providing a theoretical accuracy of under 6 metres, and Standard Positioning Service (SPS), which is slightly more inaccurate, with a theoretical inaccuracy of 10 metres. PPS is an
encrypted signal and special receivers authorised by the US military can decrypt these messages (Parkinson & Spilker, 1996).

Enhanced 911: Most of the civilian applications of GPS were initially restricted to surveying and mapping. In the US, the real driving force for the development of telematics applications has been a 1996 Federal Communications Consortium (FCC) mandate, requiring locating a caller to the emergency number 911, when the call is initiated from a wireless phone (mobile phone) (FCC-E 911, 2008). This service is called Enhanced 911 (E911). It was established because of a concern among US emergency authorities that calls from mobile phones represented an increasing percentage of emergency calls (Salmon, 2003). Many wireless operators used GPS as the positioning solution, while others used terrestrial-based techniques which are discussed in the following section. For handset-based solutions, 67% of emergency calls must be located to within 50 metres of their actual location and 95% of calls to within 150 metres of their actual location. The network-based location solutions require 67% of emergency calls to be located within 100 metres and 95% of calls to be located to within 300 metres of the actual location (Salmon, 2003; FCC-E 911, 2008; GPS, 2008).

The mandate does not specify which technology is to be used. It only defines the general specifications and the required positioning accuracy as discussed above. The E911 decision has been an important driver for the development of positioning technologies to be embedded within mobile phones. The number of GPS receivers currently embedded within mobile phones far outnumbers that in traditional GPS receivers. However, safety and security have been the main driver for mobile phone positioning in the US, in other countries it has primarily been telematics and location based computing (Rizos, 2005).
Assisted-GPS (AGPS): GPS is not capable of tracking signals of very low strengths of the order of 20-30 dB, which would be encountered inside buildings. As a result, AGPS and high sensitivity GPS receiver designs have been developed and are increasingly being deployed within mobile phone infrastructures (Feng & Law, 2002). The timing and navigation data for GPS satellites is provided by a ground station, without which the receiver would not be able to decode because of low signal strength. In short, the assistance data makes it possible for the receiver to make time measurements to the satellites, without having to decode actual GPS messages, significantly speeding up the positioning process (Rizos, 2005).

GNSS Revolution: The Russian counterpart to GPS, known as, Global’naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) was operationally falling into disrepair following the disintegration of the Soviet Union (Figure 2.3) (GLONASS, 2008). Despite constant promises by Russia to provide full operational capability,
there are only 16 operational satellites at the time of writing this thesis.

The US has so far dominated the Global Navigation Satellite System (GNSS) scene successfully, with an operationally capable system and a large user base (including civilian navigation). This dominance remained unrivalled until European Union (EU) plans were made for its own autonomous satellite navigation system, GALILEO (2007) (Figure 2.3). On November 30, 2007 the 27 EU transportation ministers reached an agreement that Galileo would be operational by 2013. The rationale for having their own system was to become less dependent on US technologically, and to deny the US dominance over military satellite navigation.

China has also recently joined the race by announcing the development of its independent satellite navigation system called COMPASS. The constellation is to consist of 35 satellites, including 5 geostationary orbit satellites (Gibbons, 2008). Japan has a system planned to provide extra GPS-like satellites called Quasi-Zenith Satellite System (QZSS) which would be a 3 satellite regional time transfer system. The first satellite is scheduled to be launched in 2009 (GPS World, 2007). India has also planned to launch its autonomous regional satellite system, Indian Regional Navigational Satellite System (IRNSS), which would consist of 7 satellites, with the first satellite launch in 2009.

The presence of many satellites would allow future GPS receivers to compute their positioning solutions by using signals from up to 75+ satellites at one time, and would improve the reliability and accuracy of computed positions. Naturally, this helps in further realization of telematics for the mass market.

Other Positioning Techniques

Despite the revolution in satellite-based positioning, GPS is not particularly suited to the urban canyon and indoor environments. For this reason several other positioning technologies are being developed which would compete/complement GNSS-based positioning.
Alternative positioning technologies use wireless communication signals or broadcasting signals. These include mobile phone signals, radio or TV signals, WiFi, Bluetooth, Radio-Frequency Identification (RFID) (discussed in Section 2.3.2 as a communication protocol), Zigbee, Ultra Wide-band (UWB) etc. A range of mathematical techniques can be applied, based on the type of measurement, including Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), Cell Identification (Cell-ID), as well as a combination of these (Raper, Gartner, Karimi, & Rizos, 2007).

Non-signal based techniques include inertial sensors (accelerometers, gyroscopes), digital compasses, barometers and pedometers. Accelerometers and Gyroscopes can also be integrated into GPS receivers assisting during periods of signal absence.

There are also non-conventional techniques which are increasingly being used to identify a person or vehicle, such as, ETC systems and surveillance technologies like Closed-circuit Television (CCTV) and ANPR. These systems match the location or last known location of the individual on the basis of their toll tag transaction, CCTV recording, or ANPR photograph. These systems could alert the authorities of a ‘person of interest’ as the vehicle or individual passes a certain area, or could be retrospectively mined for information.

2.3.2 Communications

The field of telecommunications has undergone significant changes in the last 30 years. Analog communications has gradually been replaced by digital communications and circuit switching technology has been replaced by packet switching. Another significant revolution in communications has been the development of wireless telephony (mobile phones). Mobile phones now play an important role in telematics systems, where the position of the vehicle is transmitted back to a server in order to gain access to services.
Short Message Service (SMS)

Telematics-equipped vehicles usually have an on-board Global System for Mobile Communications (GSM) chip for bidirectional communication between the telematics server and the car (Figure 2.4). SMS is the communications protocol of choice in these systems, allowing the interchange of text messages between the devices. SMS technology has facilitated the development of telematics significantly, and is used for sending notifications back to a vehicle, or sending location updates or related information and queries from the vehicle back to a central processing server.

SMS was originally proposed in the GSM series of standards more than two decades ago, as a means of sending messages to and from GSM mobile handsets. This support was later expanded to Code Division Multiple Access (CDMA), Digital AMPS, satellite as well as wired networks. Most SMS messages are mobile-to-mobile text messages, though the standard supports other types of broadcast messaging as well.

General Packet Radio Service (GPRS)

GPRS is a best-effort, packet-oriented mobile data service for users of GSM systems (Figure 2.4). It provides data rates from 56-160 kbit/s. It can be used for accessing emails or the internet where mobile and data transfer is charged per Megabytes (MB) (Nanda, Balachandran, & Kumar, 2000).

Radio Data System Travel Message Channel (RDS-TMC)

RDS-TMC is a technology for delivering realtime traffic, travel and weather information to in-vehicle navigation devices, and is typically digitally coded using Frequency Modulation (FM) radio broadcasts, as shown in Figure 2.4. Data messages are received silently and decoded by an RDS-TMC-equipped car radio or navigation system. Its implementation is being managed by Traveller
2. Telematics Concepts

Figure 2.4: Message exchange between telematics provider and subscribed vehicle.

Information Services Association (TISA), a not-for-profit company which aims to ensure an international framework and standardisation of this technology.

RDS-TMC integrates traffic data into navigation devices to dynamically re-route, on the basis of real-time accident information. Each traffic incident is broadcast as an RDS-TMC message containing an event code, a location and time of the event. This information is usually sourced from police, traffic cameras and floating car data. Location code tables are maintained with a number given to different locations on the road network, which are integrated in the GPS navigation devices. In Australia at least two companies are using this technology to broadcast traffic data to subscribed customers (Intelematics, 2008; MyRate, 2008).
RFID technology has slowly permeated many areas of life. RFID is primarily an identification technology, whereby a unique Radio Frequency (RF) signal emitted by the transmitter identifies the device. Applications such as toll collection, authentication, passport control, tracking library books, animal tracking, keyless vehicle entry, supply chain management and asset tracking have increasingly been embracing this technology (Landt, 2005). RFID implantable chips are now also being used in humans to gain access to locations, such as night clubs, and to use for paying for drinks, or opening vehicle doors or doors at home, without the need to carry a key (Masters & Michael, 2007). Experts have warned about the risk of using RFID for authentication because of the risks of identity theft.

The origins of RFID can be traced back to World War II, when Identification, friend or foe (IFF) transponders were installed on allied war-planes which emitted RF signals, to distinguish them from enemy war-planes (S. L. Garfinkel & Holtzman, 2006). In the 1970s the first technology patent appeared that could be termed the ancestor of modern RFID chips (Landt, 2005).

RFID systems consist of two main components: the RFID tag (or transpon-
2. Telematics Concepts

der), which is usually placed on the object to be identified or tracked, such as a vehicle’s toll tag, and an RFID reader (or transceiver), which is able to both read data from and write data to the transponder, e.g. the reader at the toll gantry. Further, the RFID tag contains at least two parts, the first being an Integrated Circuit (IC), for storing and processing information, and modulating and demodulating the RF signal. The second part is an antenna for reception and transmission of the signal (Finkenzeller, 1999). In Figure 2.5 an electronic toll tag, with an RFID chip and a AA battery is shown.

There are three different variants of RFID tags: passive tags, active tags and semi-passive tags. Active transponders have an on-tag power supply, and actively send RF signals when interrogated by a transceiver, while passive tags obtain all of their power from the interrogation signal of the transceiver and either reflect or load modulate the transceiver’s signal for communication. Semi-passive tags are similar to active tags in that they have their own power source, which however only powers the microchip and does not power the broadcasting of the signal. In terms of transmission of their signal, they resemble passive tags, where RF energy from the reader powers the transmission signal (Juels & Pappu, 2002).

As mentioned earlier, the unique signal that an RFID tag emits identifies it to a transceiver. This identification feature can both serve in positioning as well as communication contexts. A RFID device can also serve as a tracking tool if it is successively read by transceivers strategically placed at different locations.

2.3.3 Computing

Initially, computers were an accessory in the home or office. The miniaturization of computing devices has led to their portability and mobility. New terms like ubiquitous computing (Weiser, 1999), pervasive computing (Hansmann, Stober, Merk, & Nicklous, 2003), ambient intelligence, ‘the internet of things’, and more recently, ‘everyware’ (Greenfield, 2006) have been coined, for computing
devices that weave themselves into the fabric of everyday life. All these developments have been driven by the reduction in cost, size and power requirements of computers, and their ability to interact with each other wirelessly.

Almost a decade ago Clarke (1999b) recognised that these technologies are not being developed in isolation, but are converging towards the development of a ‘powerful compound’ of technologies. He envisioned that the combination of these technologies, such as mobile telephony with Personal Digital Assistants (PDAs) and portable computers with digital cameras and play-stations, would lead towards ubiquitous mobile computing and communications, as is being witnessed today.

**Context-aware Computing**

In human-human interaction, many factors support the seamless exchange of ideas, such as the richness of the language, and an implicit understanding of situational information or ‘context’ to increase the conversational bandwidth (Dey, 2001). These situational or environmental characteristics, such as location, time, identity and activity shape the decorum of a conversation. From a computing perspective, this context can be defined as follows:

> “A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user’s task.” (Dey, 2001)

When it comes to human-computer interaction, mostly only two of these contexts are available; namely identity and time. Consequently, computers are not enabled to take full advantage of the context surrounding the user to incorporate the richness of communication and produce really useful computations and services. Emergent context-aware applications aim to adapt themselves according to the context they are used in, with minimal input from the user, and are
2. Telematics Concepts

capable of examining the computing environment and can react to the changes in their environment using various sensors and actuators.

The Context-aware Car

The automotive industry has also witnessed an unprecedented use of many sensors to achieve a better understanding of the physical environment in order to improve the safety, security and experience of the motorist.

Air-bag systems sense the context of a collision, and react to the event. They use a number of related sensors within the vehicle, such as accelerometers, impact sensors, wheel speed sensors, gyroscopes, brake pressure sensors. When a ‘threshold’ is reached, the airbag control unit triggers the ignition of a gas generator propellant that rapidly inflates a nylon fabric bag.

Another recent invention is the use of Rain-sensing wipers (RSW), which are activated when it rains (RainTracker, 2008). These sensors work on the principle of ‘total internal reflection’, where an infrared light is beamed at an angle of 45° onto the windshield from the vehicle dashboard. If the glass is wet, less light makes it back to the sensor and the wipers are activated.

Parking sensors are now being installed in mid-range to small cars as a standard feature, to alert the driver of an unsafe distance from another vehicle. Most of these systems have ultrasonic sensors (and sometimes cameras) fitted to the bumpers of the vehicle, which transmit ultrasonic waves to detect obstacles near the vehicle. A controller installed inside the vehicle interprets this signal and alerts the driver with an audio tone emitted from the speakers. Some vehicles now also have rear-parking cameras that show the distance to a rear vehicle on the dashboard.

More recently, cars fitted with the Advanced Front-lighting System (AFS) are being released to the market by car manufacturers. AFS is used to activate the headlight beam in response to ambient weather and visibility conditions. There
are even plans to use GPS data to anticipate road curvature changes and use this information as an input to these systems. This system relies on electronic sensors, transducers, actuators, and auxiliary optical systems within a vehicle’s headlamp housing to switch the headlights on and off as operating conditions change.

Other context-enabled services include alarming the motorist when a vehicle’s headlights are left switched on when the ignition switches off, adjustment of the stereo sound when the vehicle enters a tunnel, intelligent keys with push button system, etc. These context-aware sensors build a better model of the environment and use it to provide useful and intuitive services by triggering or automating tasks.

Most of the sensors discussed above are now commercially available in a varied range of car models. From a research point of view there has been significant interest in exploiting contexts, such as location and surroundings, to cooperatively work with other vehicles and provide information to each other and to central servers (Vidales & Stajano, 2002; Zhang et al., 2003). This communication can be achieved via Vehicular Ad-hoc Networks (VANET), which is a form of mobile ad-hoc network and employs existing 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, and ZigBee protocols. Each vehicle equipped with VANET enables context-aware on-board systems with the ability to cooperate via wireless networks, and adapt to changing conditions and events. Information related to collision warnings, road sign alarms and in-place traffic view can be cooperatively exchanged.

The Locational Context

As indicated in the above discussion, the in-vehicle GPS receiver is also a sensor which reports on the current position of the vehicle. This information is used by the navigation system to route the vehicle from the source to the destination.
2. Telematics Concepts

Figure 2.6: Telematics in operation.

and is transmitted to the central server (on request, or periodically reported) for various other telematics services, as illustrated in Figure 2.6 and further discussed in Section 2.4.

2.3.4 Geospatial Data Management

Geospatial data is data related to natural or man-made features on the Earth. These include Points of interest (POIs) (hospitals, petrol stations, restaurants), lines (roads, rivers, or walking tracks), and areas (parks, ranges, land parcels) (Rigaux, Scholl, & Voisard, 2002). Using positioning technologies, the location of a vehicle can be identified. Once positioned, these applications need to manage the streams of spatial data, represent the data acquired, provide navigation applications, provide search retrieve functionalities, and model the geography of
the environment around the user (Raper, Gartner, Karimi, & Rizos, 2007).

The position can either be used in-vehicle, such as for navigation or could be transmitted to a server via the communications network to obtain services. The server may contain layers of attribute data as well as a Geographical Information System (GIS), capable of many operations. In-vehicle routing is performed by using the current location and the planned destination, and various optimization routines, such as the shortest distance, fastest route or avoiding tolls, may be applied, resulting in a map and driving directions (usually voice activated, but they can be textual too). The map data can either be in raster or vector format. Raster images are pre-rendered pictures, while vector data is a series of matching layers, each layer containing a specific type of information (a layer for parks, for motorways, for streets, rivers etc). Both formats can be used to display maps onto a screen. The system may also be integrated to find relevant services closest to the current vehicle location, such as the closest restaurants, nearest parking station, etc.
2. Telematics Concepts

2.4 Commercial Telematics Systems

The convergence of individual components of telematics (positioning, wireless communication, mapping, and computing) has found a natural platform - the car. Automobile manufacturers are competing to provide the best telematics platform and to increase their market-share by potentially developing a more constant revenue stream than new car sales. What was only available in luxury cars, such as General Motors (GM) Onstar (2008) or BMW Assist (2008) is also becoming available in cars targeted at the mass market. Some of these systems are discussed below.

Software manufacturers are partnering with car makers to design telematics suites. Recently Microsoft and Fiat unveiled their jointly developed ‘infotainment’ system, known as ‘Blue&Me’ (Microsoft, 2006). This system has a modular structure and allows installation and use of arbitrary services, and supports Bluetooth and Universal Serial Bus (USB) connectivity (Figure 2.7(a)). This system also offers services to track driving efficiency and CO2 emissions, which can be collected via a USB port and analyzed on a Personal Computer (PC) (Fiat, 2006).

Toyota’s ‘G-Book’ (Figure 2.7(b)) is another telematics framework that has been on the market for a while now (Toyota, 2008). They have even offered it to other car makers such as Subaru and Mazda (Subaru, 2008; Wireless Watch Japan, 2008). Apart from standard infotainment and navigation services, safety oriented services include alerting drivers to the presence of an intersection marked with a stop sign, for those intersections that have a high risk of accidents (The Auto Channel, 2007). This data is possibly sourced from insurance companies, who are also one of the direct suppliers of these telematics services (JCNetwork, 2008). This system could also automatically contact vehicle occupants when an airbag gets deployed, and dispatch an ambulance at non-response. It also provides an electronic account settlement function in-vehicle, which accepts prepaid
cards in addition to the traditional credit card payment schemes.

In summary, telematics systems are being introduced into a market with a huge clientele (standard cars) which has helped stimulate opportunities for other novel features where road risk and emissions-efficient driving are also being marketed to 'greener’ clients.

2.5 Mobility Pricing

Section 2.4 provided an overview of how the automobile has gradually evolved from an analogue machine with mostly mechanical and hydraulic components, to an electronic system containing several computerised subsystems operating in harmony with each other. Within the realms of this smart car revolution, mobility-pricing has drawn recent attention. The concept of differentiated-pricing or 'mobility-pricing' is not a new one (Vickrey, 1968). Mobility pricing means that different taxes, levies and insurance premiums charged to motorists
2. Telematics Concepts

for using the roads can be priced on the basis of actual usage (Vrhovski et al., 2004; Grush, 2005; Litman, 2001; Duri et al., 2004). Current technology makes it possible to design telematics-driven payment systems where costs accurately reflect usage. Figure 2.8 shows a conceptual user-interface of a proposed electronic parking system (Parking Angel, 2008).

Another significant motivation, given the rising levels of traffic congestion, is to apply congestion-charging of roads in central business districts as a method of reducing congestion on roads during peak hours and of encouraging motorists to have more flexible working hours (Litman, 2005). Such schemes are gradually being implemented in large cosmopolitan cities (Transport for London, 2008; Leape, 2006; Spencer & Sien, 1985; Vägverket, 2008). Actuarial principles of accurately insuring risks are also a motivation for piloting mobility priced insurance products. Additionally, electronic tolling is also evolving, where not only existing toll plazas are being replaced by exclusive cashless tolling (Besser, 2008), but even the newer ones being proposed and implemented have adapted distance-based tolling. For instance, in Australia the M7, which is a recent addition to the Sydney orbital network, uses distance-based tolling (Westlink M7, 2008).

In summary, congestion charging, distance-based tolling and PAYD insurance are new forms of pricing being introduced by different stakeholders, which include, the government, road authorities, private toll companies and insurance providers. Two of these technologies, one that is already established (ETC), and one that is slowly increasing its market share worldwide and is a fairly recent addition (PAYD), are explored below in a greater detail. Sections 2.5.1 and 2.5.2 introduce further details of the motivation, current implementation and basics of electronic tolling and mobility-priced insurance respectively, to which serve as a background for discussion in the next chapters.
2.5.1 Electronic Toll Collection (ETC)

Toll roads are at least 2700 years old, as toll had to be paid for using the Susa-Babylon highway under the regime of Ashurbanipal, who reigned in the seventh century BC. In India, before the 4th century BC, the Arthasastra notes the use of tolls. Germanic tribes charged tolls to travellers across mountain passes. Tolls were used in the Holy Roman Empire in the 14th and 15th centuries (Gilliet, 1990).

Many modern roads and bridges were originally constructed as toll roads, including the Sydney Harbour Bridge, which initially charged 6 pence for a car (Sydney Harbour Bridge, 2008). Turnpike trusts were established in England beginning in 1706 and were ultimately responsible for the maintenance and improvement of most main roads in England and Wales (Bogart, 2005).

Traditionally, toll roads have an entry toll plaza, with a number of toll booths, each with a turnpike (or a set of signals). When a motorist nears one of these booths, they pay the required toll fee to a toll booth operator, or put it in a collection bin (in case of 'exact change lanes'). Once correct payment has been received, the vehicle is authorised to pass. If the vehicle passes on a 'red signal' without paying the toll fees, then an enforcement system is activated which takes a photograph of the vehicle’s licence plate and relays it to an infringement processing bureau for debt collection.

Roth (1996) has criticised traditional tolling as being inefficient in three ways,

1. Manual toll collection requires vehicles to stop or slow down (in case of 'exact change' lanes), which raises vehicle operating costs and increases the time spent on toll roads.

2. Up to one third of the revenues can be absorbed by collection costs, and revenue theft is considered to be comparatively easy.

3. Even if toll roads are less congested than the parallel non-tolled roads,
the traffic diversion resulting from tolls increases congestion on the road system, rendering them ineffective.

ETC Background

ETC aims to eliminate delays on toll roads by allowing vehicles to pass toll gantries at highway-cruising speeds. ETC systems determine whether the cars are enrolled in the system, alert enforcement agencies to non-enrolment situations, and electronically debit the accounts of registered car owners. ETC promises alleviation of congestion problems, reduction of toll management costs, and cash-free convenience for drivers. Contracts between motorists and ETC providers in general require drivers' licence numbers, vehicle registration numbers, residential addresses, and a credit card pre-authorisation or a direct debit request, before an electronic tag is issued. Figure 2.9 shows how toll is collected electronically when a vehicle equipped with an RFID tag enters an electronic toll lane.

There are two central components involved in this system. One is the Road Side Equipment (RSE) (or toll gantry) which communicates with the On-board equipment (OBE) fitted in vehicles and requests it to send the unique identifiers either over the Dedicated Short Range Communications (DSRC) channel oper-
ating on the 5.8 GHz-6GHz frequency band (MG & Daley, 2002), or by using RFID technology. The OBE is a transponder, or an electronic tag, commonly referred to as an ‘E-Tag’ in Australia. The transponder fitted in the vehicle emits a unique identifier when a driver passes a toll gantry, to retrieve the associated contract information and debit the account with relevant toll fees. Detailed information such as date and time of passage, the location of the toll gantry and the amount of toll fee, is recorded in an electronic storage repository (a database) for invoice generation purposes and possible dispute resolution. Comprehensive information about the motorist’s movement is retained for as long as seven years.

Types of Toll Systems

Most new toll roads being proposed employ electronic tolling solutions. But there is also a trend to convert existing tolls that also accept cash, to move them to electronic tolling. For instance, in July 2007 the Sydney Harbour Tunnel became the first toll road to fully convert from cash to electronic toll collection in Australia, as opposed to toll roads that opened as electronic-only (RTA, 2007). Table 2.1 summarises the current situation with electronic tolls in Australia.

There are two variants of toll operations. The first is known as a ‘closed toll system’. In this type of system the vehicle entering the toll zone is identified (via its E-tag) and the toll charges vary, depending on the exit taken. Figure 2.10 illustrates the total toll charged for entering at point 1, and exiting at point 8 (Westlink M7, 2008) for Sydney’s distance-based toll road, M7. The description in the right pane explains that the toll is charged at 32.39 cents per kilometre, and capped at 20kms, meaning that the maximum toll payable on a trip is Australian Dollar (AUD) 6.478.
Table 2.1: Summary of electronic tolling operations in Australia.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Operating Agency</th>
<th>Location</th>
<th>Toll Applicable</th>
<th>Distance based</th>
<th>Cash or Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossCity Tunnel</td>
<td>Cross City Tunnel Consortium</td>
<td>Sydney</td>
<td>Both Directions</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Eastern Distributor</td>
<td>Airport Motorway Ltd.</td>
<td>Sydney</td>
<td>Northbound only</td>
<td>No</td>
<td>Only at William Street, City</td>
</tr>
<tr>
<td>M2</td>
<td>Hills Motorway Ltd.</td>
<td>Sydney</td>
<td>Both directions</td>
<td>No</td>
<td>Yes (cashless by 2009)</td>
</tr>
<tr>
<td>Lane Cove Tunnel</td>
<td>Connector Motorways Pty Ltd.</td>
<td>Sydney</td>
<td>Both directions</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>M4</td>
<td>SWR Operations Pty Ltd., RTA</td>
<td>Sydney</td>
<td>Both directions</td>
<td>No</td>
<td>Yes (cashless by 2009)</td>
</tr>
<tr>
<td>M5 South-West</td>
<td>RTA, Interlink Roads Pty Ltd.</td>
<td>Sydney</td>
<td>Both Directions</td>
<td>No</td>
<td>Yes (cashless by 2009)</td>
</tr>
<tr>
<td>Westlink M7</td>
<td>Westlink Motorway Ltd.</td>
<td>Sydney</td>
<td>Both Directions</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Sydney Harbour Tunnel</td>
<td>NSW Govt., Transfield Pty Ltd., Kuangai Gumi</td>
<td>Sydney</td>
<td>Southbound Only</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sydney Harbour Bridge</td>
<td>RTA</td>
<td>Sydney</td>
<td>Southbound only</td>
<td>No</td>
<td>No (converted to cashless on 28 Sep 2008)</td>
</tr>
<tr>
<td>EastLink</td>
<td>ConnectEast</td>
<td>Melbourne</td>
<td>Both Directions</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CityLink</td>
<td>Transurban</td>
<td>Melbourne</td>
<td>Both Directions</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

The second system is an ‘open toll system’, which consists of toll plazas, where all vehicles stop at various locations along the highway to pay a toll.
2.5.2 Mobility Priced Insurance

Maintaining and operating a vehicle involves a range of costs, some of them fixed and some variable. The classical insurance premium has traditionally been a fixed payment that covers the insured for a specified period, regardless of the distance travelled by the vehicle. As congestion on roads increases gradually, transport researchers are aiming to quantify insurance more accurately in an effort to encourage motorists to use roads more efficiently and reduce congestion, pollution and accidents (Vrhovski et al., 2004).

This class of insurance is generally termed 'Distance based charging' or 'mobility-
Distance-based charging converts insurance from a fixed cost into a variable one by taking into account the distance covered by the vehicle during the time an insurance policy is held by the motorist. This approach offers a positive financial incentive to motorists to save on insurance costs by driving less. Additionally, accident statistics suggest that there is a strong correlation between mileage and crash rates. Litman (2006) argues that reduction in vehicle travel can cause proportionally larger declines in crashes, since it reduces each vehicle's exposure to accidents. Approximately 70% of crashes involve more than one vehicle, which means that a reduction of 10% in a vehicle's mileage reduces its claim rate by 10%, and the total claim by as much as 17%, since it reduces risks to other road users as well.

Classical motor insurance products work on statistical data by dividing the population into different risk classes, on the basis of 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, whether the vehicle is garaged or parked off street, the vehicle's safety equipment, intended vehicle use (business or pleasure) and claims history (Athearn & Schmit, 1989). As the cost of insurance is determined in 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 in the successive year because of the claims made previously by high risk drivers of the insured group. This cross-financing of risk by low-risk drivers to high-risk drivers is known as ‘adverse selection’ (Akerlof, 1970). Additionally, research suggests that once an item is insured, there is a tendency to handle the insured good more carelessly. This phenomenon is termed ‘moral hazard’ (Akerlof, 1970).
Researchers have argued about the actuarial inaccuracies of current insurance policy design (Litman, 2003). Therefore, a shift towards insurance products where prices reflect costs would be a natural one, where personal auto insurers would deemphasize the focus from more controversial rating variables such as age, gender and geography, and start focusing on variables that directly affect insured driving risks.

Types of distance based charging

**Mileage Rate Factor (MRF):** The concept of using mileage to determine risks and therefore premiums is not a new one. It was introduced in the late 1960s by Nobel Laureate Vickrey (1968) as part of a vehicle insurance pricing reform to improve the fairness and efficiency of insurance premiums. Although mileage is an important risk factor, insurance companies have not been able to implement verifiable mileage readings because of associated costs. Existing rate structures are based on self-reported estimates of future travel which would be significantly underestimated by motorists if it reduces annual premiums. This renders mileage obtained by this method inaccurate for fair pricing purposes (Litman, 2006).

**Pay-at-the-pump (PATP):** PATP schemes typically add a surcharge on fuel sales to fund basic insurance coverage. The issue with this approach is that it does not directly incorporate drivers’ risk factor. Low-risk drivers with fuel-intensive vehicles would overpay their actuarially justified insurance costs, while high-risk drivers with economical vehicles would underpay (Litman, 2006).

**Odometer Audits:** This strategy directly incorporates mileage as a rating variable (Litman, 2007). It also utilises other rating factors to accurately charge premiums. Service personnel can be trained to audit odometers and report them
to the insurance agency securely. The insurance company can then re-adjust the premiums of the vehicle based on the kilometres driven. Besides, there are minimal infrastructure costs required to set up such a system.

**Incentive-based Reporting:** This is a voluntary, behaviour-based approach, where discounts are offered to the insured for providing details about how, how much and when their car is driven. This data is collected via a telematics device which connects to the vehicle’s On-board diagnostics port (OBD-II). This device gathers speed, time of day, and numbers of miles the car is driven. It also records hard braking and rapid accelerations. The Primary Named Insured (PNI) then has the option to view this data on a PC and then upload it to the insurers’ server to gain discounts. Cars that are driven less often, in less risky ways and at less risky times of the day can receive large discounts. This system does not collect any positional data as it does not use GPS.
GPS-enabled Insurance: GPS-enabled insurance has a GSM unit and a GPS device fitted to the vehicle. The GPS device collects positional data which is constantly transmitted to the insurance provider via the mobile network, as shown in Figure 2.11. Premiums are calculated by inferring kilometres driven and bills sent to drivers periodically (Norwich Union, 2007). GPS-enabled insurance charging is the most accurate method because it can also provide spatial characteristics in addition to the mileage, i.e. where and when the vehicle was driven.

Benefits of Mobility-Priced Insurance

Actuarial accuracy: Underwriting of insurance policies is typically done using actuarial science, which uses statistics and probability to analyse risks associated with the hazards covered. In the US, the ‘Actuarial Standards of Practice’ promulgate the standards of practice for the actuarial profession. Actuarial Standard of Practice No. 12, related to ‘Risk Classification’, says that a sound risk classification system should reflect cost and experience differences on the basis of relevant risk characteristics (Actuarial Standards Board, 1990). Mobility-priced insurance has the ability to more actuarially-accurately capture those risks which it was not possible to encompass in traditional motor insurance products.

Insurance affordability: Mobility-priced insurance has the potential to attract uninsured drivers who could not previously afford insurance. Lower income households tend to drive their vehicles less than average, so a mobility-priced system would probably be a more attractive and affordable cover choice for them (Litman, 2006).

Congestion management: Distance-based charging converts the traditional ‘drive all you can’ insurance to a system where costs reflect usage. This would
2. Telematics Concepts

courage motorists to plan their travels more efficiently, because the fixed cost of insurance is flexible now and is regulated by mileage, which would help in congestion management and to alleviate environmental issues such as stop/start and transport related pollution. It is more risky to be on roads during peak times (Litman, 2006), and as a result this class of insurance would have a higher premium per kilometre during rush hour, which would act as an incentive for users to have flexible working hours and to avoid the rush hour and thus save on insurance.

**Fairness of system:** 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. It is possible that each rating class may have both high-risk drivers as well as low-risk ones, which implies that low-risk drivers are cross-financing the claims made by high-risk drivers. Researchers have extensively debated and discussed the actuarial inaccuracies of current insurance policy designs (Litman, 2003). Therefore, the shift towards insurance products where fairness is reflected would be a natural one.

**Current Implementation**

The previous sections have covered the various methods of applying distance-based charging. It was concluded that GPS-based insurance has the capability to measure road-risks with higher accuracy than others. This section reviews some of the existing implementation of mobility-priced insurance, with a particular focus on the ones which use GPS data for processing.

From 1995 to 2005 at least 4 patents were filed in the world related to telematics-driven insurance architectures (Perez, 1996; McMillan, Craig, & Heinen, 1998; Nakagawa et al., 2002; Toshihiko, 2005). Progressive Casu-
2. Telematics Concepts

Pay As You Drive™ insurance

### Summary of usage

<table>
<thead>
<tr>
<th>Mileage covered</th>
<th>Miles per Mile</th>
<th>Premium charged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorway</td>
<td>213.9</td>
<td>1.5 p</td>
</tr>
<tr>
<td>Dual Carriageway</td>
<td>234.0</td>
<td>2.1 p</td>
</tr>
<tr>
<td>Built up areas</td>
<td>91.3</td>
<td>8.7 p</td>
</tr>
<tr>
<td>Non built up areas</td>
<td>16.0</td>
<td>8.2 p</td>
</tr>
<tr>
<td><strong>Mileage based cost summary</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Mileage based cost summary | | **£42.74** |

- **Off Peak**: £4.92
- **Weekend**: £8.00
- **Commuter route**: £12.50

| Total discounts earned this month | £21.38 |

<table>
<thead>
<tr>
<th>High risk charges</th>
<th>No. of days</th>
<th>Charge per day</th>
<th>Premium charged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rainy days</td>
<td>2</td>
<td>£1.00</td>
<td>£2.00</td>
</tr>
<tr>
<td>Ice Snow days</td>
<td>1</td>
<td>£8.00</td>
<td>£8.00</td>
</tr>
<tr>
<td><strong>Total high risk charges this month</strong></td>
<td></td>
<td></td>
<td><strong>£10.00</strong></td>
</tr>
</tbody>
</table>

| Static risk Premium | £10.00 |

| Total Monthly Usage Premium | £41.38 |
| Insurance Premium Tax (IPT) @ 50.0% | £2.07 |
| **Total insurance Premium** | **£43.45** |

Figure 2.12: A sample bill of charges for Norwich Union’s PAYD, Source (Norwich Union, 2007).

Progressive Insurance in the US invented and patented the business model of using a combination of GPS receivers and GSM mobile phones to track the movements of vehicles which are retrospectively used to calculate driver risks and premiums (McMillan et al., 1998). There is also a European patent that does not involve the use of GPS for positioning, and falls under the category of incentive-based reporting, as discussed earlier (Perez, 1996). This design utilises monitoring the car’s engine control computer - OBD-II to the determine distance driven, speed, time of day and braking force. Ironically, Progressive Insurance is developing the European patent in the US, while it has issued licences for companies in Europe and UK to implement its GPS-based design.

The first implementation of a GPS-enabled insurance product was piloted
in the UK by Norwich Union in 2005, and is known as PAYD. Customers who joined had a black box fitted in their car which constantly fed back data on their GPS locations to a central processing server. This data was used to determine where and when they were driving. Younger drivers were charged at about 5p per mile if they avoided rush hour, but at £1 a mile for driving late at night (Norwich Union, 2007). An invoice which included a detailed breakdown of the charges was mailed to customers every billing cycle. Figure 2.12 is an illustration of the summary of charges billed using the distance and time/day the vehicle was used. Although this application attracted significant initial attention from motorists with promised savings, Norwich Union only recently announced that it was discontinuing its PAYD product (Howard, 2008). There is, however, another insurance provider introducing mobility-priced insurance in the UK, known as Coverbox (2008), which works on similar principles.

In South Africa, Hollard Insurance (2008) has a GPS-based PAYD scheme which splits monthly premiums into two portions: a fixed premium, based on standard rating variables, and a variable premium, based on kilometres driven over and above the 417 km issued monthly quota. The insurance premium is capped at 3,200 km per month, meaning that if a motorist drives more than this, they will not be charged additional premiums above this threshold.

Aioi in Japan has partnered with Toyota motors and has been marketing its PAYD version since 2005. This product is based on Toyota’s G-book telematics platform (discussed earlier) and sends movement data to the insurance server for processing. Their plans calculate mileage per month and give customers the opportunity to save on premiums on the basiss of their driving habits (Aioi, 2008).

GM has an insurance program for customers who own GM vehicles and have subscribed to their OnStar telematics service (discussed above). This system automatically reports the vehicle’s odometer reading at the end of policy cy-
Motorists who drive less in a particular period receive insurance premium discounts of up to 40%, depending on mileage (GMAC Insurance, 2008).

WGV insurance group and T-Systems have piloted a GPS insurance product in Germany (T-Systems, 2006). The technical solution consists of an on-board computer installed in the vehicle by a provider. The on-board unit registers data about the car’s location based on the GPS receiver, and periodically sends this information via GPRS to a data center operated by T-Systems. This data is then further processed, and details like the distance driven, time of day and the roads taken are provided to the insurance provider. Instead of disclosure of the whole GPS log, only processed data is transmitted to the insurer.

**Situation in Australia**

In the Australian context, a recent statement by a National Roads and Motorists Association (NRMA) 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).

The current implementations of GPS-GSM architectures may not be entirely applicable to the vast continent of Australia. Spatial maps of GSM coverage of Australia show that it is possible to have no network coverage when travelling between two remote towns in the Australian outback (GSM World, 2008).

That is probably why the first PAYD product introduced in Australia does not depend on GPS/GSM for generating mileage-based premiums. Real Insurance (2008) has taken the simplest approach, using MRF, and relies on the estimated kilometres reported by customers that they intend to use their vehicles for. There is a base rate and a minimum of 5000 KM that customers pre-purchase. The unused KMs are carried forward or if the estimated mileage is used up, customers can purchase more KMs over the phone using a credit card, much like prepaid mobile phone cards.
2.6 Summary

This chapter has introduced the field of telematics and outlined the important convergent developments that have created novel opportunities in the transport telematics arena. All these developments have made the concept of mobility-pricing a reality, where motorists are offered the opportunity to convert some of their fixed costs, such as insurance and road tax, to variable ones, depending on how, when, and how much they drive. The location of the vehicle plays a critical role in the development of mobility-pricing services. It has also been established that the GNSS revolution would be beneficial in further improving the availability and reliability of these systems.

With every opportunity there are associated risks, and so the next chapter looks at some of the social impacts of the electronic pricing of road usage which have emerged as a result of the availability of precise location information.
Chapter 3

Location Privacy Concepts

This is a free country, madam. We have a right to share your privacy in a public place. – Peter Ustinov (Romanoff & Juliet, 1956)

3.1 Introduction

The converging technologies of communication, positioning, computing and geospatial data management give reality to the telematics vision. While these technologies have revolutionised the way we interact with machines and with each other, they pose certain challenges to the location privacy of citizens. This chapter introduces privacy concepts and reviews the issues associated with location privacy within philosophical, social, legislative, and technical contexts. Section 3.2 and 3.3 provides a background to privacy and associated concepts. Section 3.4 delves more deeply into defining location privacy and its telematics related issues. Section 3.5 explores the issues of trust and ethics, survey research, and the social norms of location privacy. Section 3.6 evaluates the current situation in terms of legislative frameworks and case law, while section 3.7 reviews current work on location privacy.
3.2 Privacy Concepts

3.2.1 History of Privacy

"O ye who believe! enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you, in order that ye may heed (what is seemly).

If ye find no one in the house, enter not until permission is given to you: if ye are asked to go back, go back: that makes for greater purity for yourselves: and God knows well all that ye do." Al Qur'an, 24 (27-28).

The right of privacy, which was not recognized in Western legal traditions until modern times, has recognized in Islamic law since the beginning of Islam (Weeramantry, 1988, p. 136-137). Approximately 1400 years ago, the distinction between public life and private life was made in Al Qur'an in numerous verses. Visitors were warned not to cast curious gazes inside other people's homes when they came to visit and waited outside (Saad, 2008).

Recognition of privacy is also deeply rooted in other religious scriptures and ancient societies. For instance, the Bible has numerous references to privacy (Moore, 1984; Hixson, 1987), and notions of privacy can be identified in classical Greek and ancient Chinese societies too (Privacy International, 2007).

In more recent Western societies the 18th Century British statesman William Pitt declared in a speech before Parliament,

"The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail: its roof may shake: the wind may blow through it; the storms may enter; the rain may enter, but the King of England cannot enter: all his forces dare not cross the threshold of the ruined tenement" (Strum, 1998).
3. Location Privacy Concepts

When the US constitution came into effect, it contained 10 amendments, called the Bill of Rights. The Fourth Amendment states that,

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (Ducat & Chase, 1992)

The historical and philosophical pronouncements cited above underline the 'your home is you castle' idea, declaring privacy to be a fundamental human right (Henderson, 2006).

3.2.2 Privacy in the Modern World

Definitions

It has been said that privacy is ‘notoriously, even impossibly difficult’ to define (Foord, 2002). Obtaining a definition for privacy, rather than producing abstracted generalisations has been recognised as difficult (Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd. 2001). Even though privacy is ill-defined, it is apparently a well-understood concept in the sense that most people use this term believing that others share their particular definition (Waldo, Lin, & Millett, 2007). Nonetheless, it is important to quantify what privacy is in the context of this thesis.

Privacy a right: Warren et Brandeis (1890) argued for a right to privacy in the Harvard Law Review. In their seminal piece on the right to privacy, they defined privacy as ‘The right to be let alone’ (Warren & Brandeis, 1890). In the US, the concept of this privacy right gradually became part of common law.
At an international level, the 1948 Universal Declaration of Human Rights specifically protects the right of privacy. Article 12 states:

“No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.” (Universal Declaration of Human Rights, 1948)

**Privacy as a claim:** With the arrival of information technology, the interest in the right of privacy increased. The power of storing information about individuals demanded more specific rules governing collection and handling of personal information. Westin (1967), defined privacy in informational contexts as follows:

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

**Privacy as an interest:** Clarke (1999a) has argued that if privacy is claimed to be a right, it is easily confused between legal and moral rights - as a right implies an intrinsic and absolute standard, something not always applicable to privacy. He therefore defined privacy as

“the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations.” (Clarke, 1988)

This thesis uses this working definition of privacy as it caters for more flexibility in defining personal space in a world where cyberspace so often intersects physical space.
3.2.3 Various Facets of Privacy

In general privacy can have four separate but related aspects. (Australian Law Reform Commission, 2007) as discussed in the following subsections.

**Bodily Privacy** Bodily Privacy concerns the integrity of the individual’s body against compulsory invasive procedures or procedures performed without consent.

**Territorial Privacy** Territorial Privacy concerns the setting of limits on intrusion into the domestic or other environments, such as workplace or public space, including searches, video surveillance and ID checks.

**Informational Privacy** Informational Privacy or data protection involves establishment of rules governing collection and handling of personal data.

**Communications Privacy** Communicational Privacy concerns the security and privacy of mail, telephones, e-mail and other forms of communication.

3.3 Important Concepts Related to Privacy

3.3.1 Surveillance

The word ‘surveillance’ in French means ‘watching over’, which could be used for control, entitlement, management, influence and protection (O’Hara & Shadbolt, 2008, p. 26). The terms is often used for all forms of observation and monitoring, not just visual surveillance. Lyon (2001) defines surveillance as being

"the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction." (Lyon, 2001, p. 2)

Lyon (2001, p. 1) further adds that all societies using communication and information technologies for administrative purposes are essentially ‘surveillance societies’. In recent years, surveillance technologies are increasingly being used
as a deterrent to criminal activity, as a tool for prevention, detection and interception of unlawful activity, as a tool in investigations, and as a confidence building measure for the public (Wigan & Clarke, 2006).

However, the negative impact that surveillance has on the autonomy and privacy of individuals sometimes outweighs the benefits. This tension between community trust and the effectiveness and deterrence aspects of surveillance have to be finely balanced (Wigan & Clarke, 2006).

Surveillance can be further divided into two types, ‘personal surveillance’ and ‘mass surveillance’. As these names suggest, personal surveillance relates to surveilling identified persons. There would be a specific reason for investigation or monitoring in this type of surveillance. Mass surveillance is the surveillance of groups of people, where the reason to surveil would be to identify individuals belonging to a particular class that the surveilling party is interested in (Wigan & Clarke, 2006).

In transport contexts, CCTV surveillance constitutes mass surveillance, whereas red-light camera or speed cameras are activated on an event, and are there to collect evidence of a personal infringement. A recent example of mass surveillance projects in Australia includes CRIMTRAC’s proposal to employ ANPR technology, which, when fully functional, would take up to 70 million high resolution pictures every day of not just the licence plates, but also the front seat occupants of vehicles (Dearne, 2008). These cameras would be placed on up to five thousand strategic road locations all over Australia. It is initially planned that these photographs would be retained for a period of five years and data-mining technologies would be employed for retrospective analysis (CRIMTRAC, 2008).
3. Location Privacy Concepts

3.3.2 Dataveillance

As governments and organisations continue to increasingly store information about individuals, surveillance of a new kind has become feasible. This new technique has the capability to detect error and fraud in large-scale systems. However, in doing so, it also intrudes on the information privacy of everyone whose data is involved in this exercise, significantly altering the balance of power between the concerned parties (Clarke, 1994). Clarke (1988) coined the term data surveillance, or 'dataveillance' which refers to the use of personal data in monitoring actions of communications of individuals, and is defined as

"systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."

(Clarke, 1988)

Most mobility-pricing systems use GPS logs to calculate the distance travelled on different types of roads in order to invoice customers. These GPS logs are disclosed to the pricing server using the GSM network. GPS logs are a form of data, and their monitoring falls within the realms of the aforementioned informational surveillance or dataveillance. On the other hand, ETC systems collecting information about the passage of subscribed vehicles at different toll gantries also register data about the vehicle’s identity, time, date and location of passage into its own database for payment enforcement.

This data can be mined using data-mining techniques to create profiles of patrons, which can be sold to other agencies, for instance to insurance companies. Wigan et Clarke (2006) have pointed out that this data can also be used to infer social networks. They argue 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, and probabilistically infer social networks.
3.3.3 Überveillance

M.G. Michael builds on the concept of dataveillance and proposes a new term, 'überveillance' to define how pervasive computing and ubiquitous computing concepts (discussed in Chapter 2) have also enabled 'an above and beyond almost omnipresent 24/7 surveillance' (K. Michael, McNamee, & Michael, 2006). He further adds that überveillance creates several issues of grave concern, such as the possibility of misinformation, misinterpretation and information manipulation.

Überveillance has the capacity to not only automatically identify people, but to also automatically locate them in an attempt to verify current or planned activities. Hence it can be a predictive mechanism for one's behaviour, characteristics, and personalities (M. G. Michael, Fusco, & Michael, 2008). In locational contexts, inspecting one's historical or current movement may be used to make inferences about the individual. However, as Michael acknowledges, there might be false positives as it is not necessarily true that facts add up to the truth, since predictions based on intelligence are not always correct.

As discussed in the previous chapter, technology is taking a new turn by convergent technologies of mobility, connectivity and computing. The opportunities in the field of telematics have already been reviewed. The associated threats require immediate attention, because of the nature of transformation of data collection from being static and discrete, to becoming highly automated, embedded and updated and based on various events and contexts (M. G. Michael et al., 2008). These technologies of surveillance are becoming less obvious and overt, but more systematic and subtle (Lyon, 2001, p. 2).

3.3.4 Tracking

Clarke (2001) defines tracking as

"... the plotting of the trail, or sequence of locations, within a space..."
that is followed by an entity over a period of time. The 'space' within
which an entity's location is tracked is generally physical or geographical; but it may be virtual."

Visualising the tracks, routes and waypoints on a map obtained from a GPS receiver is referred to as GPS-tracking. It is important to understand that a GPS device installed in a mobile-phone or in a vehicle may be able to compute its position on the basis of available satellite signals and record or self-report the position and elevation. GPS is not in itself a surveillance or tracking mechanism. The core issue is access to this data, either via continuous or periodic transmission via a communications channel or retrieval from a device, without the consent or will of the person whose movements have caused the GPS device to record positions. The distinction between this data-generator and the owner of this device is important as they may be different individuals, and the data-generator may not be aware of their movements being recorded and retrieved by someone else.

3.3.5 Anonymity

‘How anonymity exists? It exists because people are not engineered
to remember, but are designed to forget’ (Coney, 2006).

When the notions of privacy developed in Section 3.2.1 are applied in public spaces, anonymity plays an important part. People, when in public places such as roads, parks, streets or markets, are aware that they can been seen by others and in turn can see others. However, the key to understanding anonymity is the inability of individuals to record everything that they see and to recall it in great detail at a later date.

While drivers are rarely completely anonymous because each registered vehicle has a unique licence plate issued by the motor registry, which the motorist
is required by law to display on both the front and rear of the vehicle, motorists have been able to travel fairly anonymously on roads until recently. Motorists also appreciate that anonymity is momentarily or temporarily lost if they are reckless, such as near a speed camera, or a red light camera.

### 3.3.6 Identity

If anonymity lies at one end of the spectrum, identity lies at the other. Personal identity is the way in which a person defines themselves in terms of their individuality and differences from others. Part of it is given at birth, via a birth certificate, a name, gender and nationality. Other aspects of this identity are formed as people grow, mature, and make choices, forge relationships and build an evolving identity.

Anonymity is the state of being unidentified by observers, while identity is the opposite state, where observers identify us based on certain characteristics. Privacy is the interest by individuals to be in control of information about themselves. People use this interest to regulate where they are or want to be positioned on the anonymity spectrum; when to assert privacy or when to forego it, depending on the costs and benefits of doing so.

As mentioned earlier, drivers are not completely anonymous: they display their licence plates, which are observable by other motorists in close proximity. This trend is changing with the systematic demand for retention and processing of identity from motorists for road pricing and other agendas.

### 3.4 Location Privacy

A classification of privacy based on its facets has been described in Section 3.2.3. It is clear that 'Location privacy' is multi-faceted and includes territorial, informational and communicational privacy. It involves communication, since a
vehicle and RSE interact with each other, and there is a mutual interest that
this communication remain private. It involves information privacy, since there is
transmission of data between these entities, and each transmitted chunk of data
is identifiable, or can be related to the vehicle and its owner. It also involves
territorial privacy, since observations made on a GIS map of the current location
of the vehicle, or the images photographed at toll gantries mark the territorial
boundary of where that information originated from.

3.4.1 Definition

Using Clarke’s definition, a modified definition for location privacy would look
something like:

“the interest that a ‘motorist’ has in sustaining a ‘personal locational
space’ free from interference by other motorists, telematics providers
and other organisations.”

The reason for this specificity of identifying the stakeholders as well as the
spatio-temporal personal space is that they are an important aspect of location
privacy in telematics, where identity, activity, time and place are key factors.

3.4.2 Location Privacy Classification

A privacy classification of location information is presented in this section. For
this purpose it is important to understand the concepts of personal information
and sensitive information first.

According to The Privacy Act 1988 (2009), personal information means ‘in-
formation or an opinion (including information or an opinion forming part of a
database), whether true or not, and whether recorded in a material form or not,
about an individual whose identity is apparent, or can reasonably be ascertained,
from the information or opinion.’ This means information that can be related to
a specific individual such as date of birth, gender, address. Collection, storage, and use of personal information is governed by the Privacy Act.

Sensitive information is a subset of private information that has additional protection under the Act under NPP 10, and generally requires consent (exceptions include being required or authorised by law) without which an organisation is not allowed to collect this information. Sensitive information includes racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, sexual preferences or practices (National Privacy Principles, 2001).

Based on this distinction, the following is a possible classification mechanism,

1. **Location Information**: Geographically referenced data with no personal information.

2. **Personal Location Information**: Geographic component along with personal information, such as land titles.

3. **Personally-sensitive Location Information**: Geographic component revealing sensitive personal information such as ethnicity, sexual orientation, etc.

Figure 3.1 illustrates the different types of location information. There are blurred boundaries in this attempted classification, because at times location information, with no overt identification information, could be used to identify a living person. Residential address may only be considered location information until it is used to identify an individual. For instance, if there is only one individual living at a property in an isolated area, the street address can be used to reasonably infer the identity of this person.

In addition, it is also possible to infer sensitive details about individuals on the basis of their personal location information because of the ability to make
selective inferences with location information. These inferences can create new information. Some of this newly generated information may reveal sensitive private information, such as political affiliation, religious beliefs or sexual orientation, which would be in direct violation of NPP 10, as mentioned earlier, requiring the explicit consent of the data subject when collecting sensitive information. Locational privacy is particularly challenging, because much debate about privacy has traditionally been characterised in terms of the identity and activity of an individual, rather than their location (Clarke & Wigan, 2008).

### 3.4.3 Telematics & Privacy

More than a decade ago, when ITS and telematics technologies were in their nascent stages, Agre et Harbs (1994) in their illuminating article voiced concerns about the ability of driver pattern data to be collected, and the temptation of using this for secondary purposes. These issues have now become a reality.

Telematics technologies that cannot or do not specifically identify a vehicle
or driver raise few, if any, privacy issues. However, some transport telematics technologies pose a significant threat to the privacy of individuals. The extent to which privacy concerns are evoked depends on a number of factors related to what information is collected, how it is stored, and how it is used (Briggs & Walton, 2000). Table 3.1 summarises some transport related applications that have the potential to alter the balance of privacy on roads.

Telematics technologies pose a challenge to two different dimensions of privacy. The first is the threat to autonomy and anonymity because of increasing surveillance, and the second is the resulting loss of information privacy. These technologies can hinder personal autonomy because of their capacity of surveillance and monitoring. Some of these applications may provide journey patterns to interested parties such as government private organisations. Notions of privacy also include the individual’s interest in controlling or participating in decisions about the use of their own personal information (Intelligent Transport Systems, 1996).
3. Location Privacy Concepts

Table 3.1: ITS technologies with potential privacy concerns.

<table>
<thead>
<tr>
<th>Transport Application</th>
<th>Primary Data Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Clearance Systems</td>
<td>These systems utilise Advance Vehicle Identification (AVI) technology, databases for carrier safety and credentials to electronically clear commercial vehicles at border crossings.</td>
</tr>
<tr>
<td>Electronic Toll Collection</td>
<td>ETC electronically deducts toll by identifying a vehicle with its E-Tag.</td>
</tr>
<tr>
<td>Electronic Enforcement Applications</td>
<td>These devices include, red light cameras and speed cameras and allow for automated enforcement of traffic violations.</td>
</tr>
<tr>
<td>Vehicle Probe Applications</td>
<td>These are technical applications used to detect and track individual vehicles for research purposes and for abstracting traffic characteristics, such as trip origins and trip destinations.</td>
</tr>
<tr>
<td>Video Surveillance Applications</td>
<td>Video cameras are used for a number of purposes, from visual surveillance of traffic flows, to identifying a particular vehicle.</td>
</tr>
<tr>
<td>Vehicle Telematics Systems</td>
<td>Private vendors and automobile manufacturers now equip vehicles with telematics systems, with the capability of bidirectional communication between the vehicle and a base-station</td>
</tr>
<tr>
<td>Event Data Recorders</td>
<td>Most new vehicles are fitted with trip computers and data recorders (similar to black boxes in aircraft), which record the characteristics of the engine, braking and safety systems.</td>
</tr>
<tr>
<td>GPS-priced insurance</td>
<td>Mobility-priced or GPS-enabled insurance, where premiums are calculated based on vehicle usage.</td>
</tr>
<tr>
<td>Mobile-phone based positioning</td>
<td>Mobile phones with GPS and AGPS capabilities can pinpoint accurate location. New applications such as Google Latitude, which uses Google Maps and a geo-coded cell-tower database to infer current position.</td>
</tr>
<tr>
<td>ANPR</td>
<td>These devices are quite similar to red light cameras or speed cameras, which is a mass surveillance method that uses optical character recognition on images to read the license plates on vehicles. It is not triggered by an event such as speeding, rather it records all movements.</td>
</tr>
</tbody>
</table>
3.5 Social Mechanisms for Privacy Protection

Socio-economic activities have attracted more and more people to cities, resulting in the metropolises witnessed today. When people lived in small towns, there was less movement and there was little privacy, as most people were identifiable and their activities were observable by others from the town. Yet there were social mechanisms present that prevented abuse of privacy (Wright, 2002).

On the other hand, the transmigration to bigger cities brought increased mobility and an increase in the ability to remain anonymous. However, social mechanisms reduced (Wright, 2002). With current mobile societies, with technologies that are able to identify and track individuals, a new change is being witnessed, one where social mechanisms and privacy are both greatly reduced.

3.5.1 Ethics

The word *ethics* originates from the Greek word *ethos* which means *character*. The word *morality* comes from the Greek word *mores*, meaning *social rules* or *customs* (Gert, 1998). The meanings of these words are often reversed in the modern world, with morality governing personal behaviour, and ethics referring to the external science of moral values and theories (Langheinrich, 2005). Ethics is quite relevant to privacy, because it provides the distinction between what is appropriate and what is inappropriate, and can have a strong influence on human judgement of privacy violations.

If future smart home appliances are to be required by law to report unlawful behaviour, such as storing explosives in the freezer, or watching videos which incite violence, how would individuals react? This spy in the home would not disclose any lawful information, only major crimes such as murder or terrorist activity. A question that needs to be asked here is which conception of established moral values apply in this case? (Langheinrich, 2005).

K. Michael et al. (2006) have proposed an analysis framework to evaluate the
ethical issues of GPS monitoring. They 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. This study classified current GPS applications into the contexts of control, convenience and care, and used the criteria of privacy, accuracy, property and accessibility for gauging the viability of a Location Based Services (LBS) service. Their research identifies the ethical dilemmas associated with the use of GPS on civilians and shows that adequate safeguards need to be in place to avoid abuse of information gathered through GPS technology.

### 3.5.2 Trust

Trust is related to the assumptions one makes about others after exposing one’s vulnerabilities to them, believing they will not take advantage of this knowledge by revealing it to others. The trust at play between people, and between people and machines, is an important social mechanism. Disclosure of private information to another person or entity hinges on trust. By placing trust in others, one grants them the option of violating this trust, while expecting them not to do so (Langheinrich, 2005). In other words, it means having faith in somebody. Trust has received considerable attention in the fields of social science, literature, psychology, sociology and political science (Langheinrich, 2005). Trust is closely related to autonomy, independence and freedom.

Trust is an important aspect in the functioning of society. Self-respect and trust are also closely related: lack of trust in others means a lack of respect for others. Applications utilising the location of the individual for providing services pose a threat to the maintenance and propagation of trust (M. G. Michael et al., 2008).
3.5.3 Societal Norms

Privacy researchers have attempted to build a theory of privacy in public by drawing on existing legal frameworks and philosophical contexts (Nissenbaum, 1997, 1998; Allen, 1998; Slobogin, 2002). These theories fall short of questioning public surveillance in non-intimate circumstances and of asking what morals guide such surveillance.

Nissenbaum (1998) cites three factors, namely conceptual, normative and empirical, that contribute to the general disregard of privacy in public. Conceptually, the notion of privacy in public has been considered paradoxical because of the attempts to demarcate it into a private/public dichotomy. This theory marks two mutually exclusive spheres of intimate and non-intimate information, which has been an effective tool to keep privacy-violators out of the private sphere. An example of this concept is that adversaries may not have a right to eavesdrop on conversations taking place in the house, but it is perfectly legitimate to note down a driving vehicle’s licence plate details. Personal privacy is voluntarily relinquished by allowing bodily searches in the interest of security when boarding a plane. Privacy in public has not gained much attention by privacy theorists, because prior to key developments in information technology the issue of mass scale surveillance was never experienced to the extent that it is present today. One reason for this is the exponential decline in data storage costs, coupled with huge increments in computing power, which has enabled devices capable of performing pervasive surveillance.

Nissenbaum (2004) further argues that a new approach is required to tackle the complex issue of privacy in public, and proposes the theory of ‘contextual integrity’. This theory is built around the notion that all realms of life are governed by norms of information flow and consist of two types of norms: norms of appropriateness and norms of distribution. Norms of appropriateness distinguish between intimate information that it is appropriate to disclose, and information
that is inappropriate. In a financial context, it is appropriate to divulge information about salary and current savings to a financial advisor when applying for a loan, but it may not be appropriate to discuss details of a romantic relationship. 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 they disclosed this information to a third party.

Contextual integrity, according to Nissenbaum (2004), is maintained when both the norms of appropriateness and norms of distribution are respected.

Zinner (2005) builds upon her work, and applies the theory of contextual integrity to the vehicular technology environment. He argues that vehicles on roads are publicly observable, so it is appropriate for a passer-by to observe their surroundings. Similarly, it is appropriate to observe the contents of the licence plate of a vehicle as it drives past an individual, as these are publicly displayed. Observing all vehicles on all roads at the same time, and recording their details are natural barriers for an observer, which prevents mass surveillance and constitutes the norms of distribution in transport technology.

Recent developments in transport technology with the agenda of enforcement, policing, road safety and road pricing have initiated a disruption of these norms. Now it is possible to perform both mass surveillance as well as personal surveillance of vehicles, using systems such as E-Tags, without being in close proximity to a vehicle, and without the need for a human performing such surveillance. Norms of appropriateness may be disrupted by E-Tag systems, where it is possible to identify a vehicle with precise details, such as its vehicle identification, heading, the day and time it passed a particular and successive toll booths, and possibly a picture of the vehicle’s licence plate. Further, these systems enable storage of this information for later review, analysis and distribution, disrupting the norms of distribution.
3.5.4 Social Survey Research

Within the area of location-privacy, various surveys have been conducted to seek an understanding of how much users value their location information. Some studies have sought to determine the monetary value that would attract a person to disclose their location information, while others have focused on the social networks that people would be comfortable in disclosing their whereabouts to.

Danezis, Lewis, et Anderson (2005) conducted an experiment with undergraduate students at a university campus in which they explained to potential respondents that their mobile cell location information would be used for a period of 28 days at a 500m resolution in exchange for financial incentives, and selection of candidates would be based on a reverse auction sequence. Potential respondents were asked to go online to a portal and make their bids about how much compensation they expected for disclosing their location data for the length of the required study. The bids ranged from £0 - £400 with a mean value of £27. This study provides a measure of personal privacy, but the authors of this study acknowledge that this value may be a lower bound on the value of user's location information, as a typical undergraduate student may have a greater desire to sell his/her information at a cheaper price than the general population.

Barkhuus et Dey (2003) also conducted a series of experiments in an attempt to gauge how students rated ubiquitous services for usefulness and intrusiveness. Four hypothetical services, among which two were location-tracking and the remaining two position-aware, were provided to the users for use on their mobile phones. Position-aware services computed the position on the mobile phones independent of the network, while the location-tracking services notified an interested party once the user's mobile phone was within a predefined region. Interviews conducted with the participants revealed that people were more concerned about being tracked than when their mobile phone reacted to a change
in location. Nearly one-third of the participants said that they would never use location tracking applications because of their intrusive nature.

In the context of social disclosure of location, a study was conducted to understand whether and what users are willing to disclose about their location to social relations (Consolvo et al., 2005). With the 16 nontechnical participants recruited, a three-phased study was conducted. In the first phase the study investigated the structure of participants' social networks. In the second and third phases they studied how participants responded to hypothetical location requests from their social relations, and their reflection on these experiences in location-enhanced computing respectively. The study concluded that location disclosure depended on aspects like granularity of information sought, the relationship with the requestor, the location of the requestor, the location of the participant and the activity of the participant.

3.6 Legal Mechanisms for Privacy Protection

Explicit legal protection for location privacy is not consistent across the world. This reflects differing levels of views, awareness and concern among policy makers, analysts and privacy advocates. There are no specific provisions in Australian and New Zealand privacy legislation specifically addressing location privacy. Telecommunications legislation covers inappropriate disclosure of location information for mobile phone usage (Caslon Analytics, 2008). The following sections give a brief overview of the legislative instruments in Australia and other jurisdictions, which is followed by an examination of case law from various jurisdictions related to location privacy.
3.6.1 Legislative Frameworks

Legal Instruments in Australia

Privacy Law in Australia comprises several Commonwealth laws which cover public sector and most private sector activities, some state and territory laws, and the remaining common law protections (Privacy International, 2004). There had been no recognition of a tort of privacy until recent recommendations by the Australian Law Reform Commission (ALRC) for such a tort (Australian Law Reform Commission, 2008).

The principal federal statute is the Privacy Act of 1988 (The Privacy Act 1988, 2009), which emerged as Australia’s commitment to the Organization for Economic Cooperation and Development (OECD) guidelines and the International Covenant on Civil and Political Rights (ICCPR) Article 17 (Privacy International, 2004). The Privacy Act provides a set of eleven Information Privacy Principles (IPP) applicable to most federal government agencies, and a set of ten NPP which is applicable to most private sector organisations as summarised in Table 3.2 and extracted from National Privacy Principles (2001).

States and territories in Australia have varying privacy laws. New South Wales (NSW) passed the Privacy and Personal Information Protection Act 1998 (NSW), which applies to most state government agencies. This Act does not specifically contain an anonymity principle such as the NPP. Victoria enacted the Information Privacy Act 2000, which is the primary privacy legislation for Victorian state government agencies. In Queensland, no privacy legislation exists; there is only an Information Standard. The Solomon Report on the Right of Information made recommendations for privacy and the Queensland premier has committed to an Information Privacy Bill. Tasmania enacted the Personal Information Protection Act 2004. It establishes a set of ten Personal Information Protection Principles (PIPP). They apply to Tasmanian government agencies, but with many exemptions and exceptions. The Northern Territory
In addition to these privacy laws, a complex mix of privacy standards applies to the telecommunications industry. The Telecommunications Act 1997 contains a list of exceptions from a basic presumption of confidentiality of customer records, and is similar to the disclosure principles of the Federal Privacy Act. The enforcement position is confusing in the telco sector with the Australian Communications and Media Authority (ACMA), the Privacy Commissioner and the Telecommunications Industry Ombudsman sharing overlapping jurisdictions (Privacy International, 2004).

The Telecommunications Interception Act of 1979 regulates the interception of telecommunications. A warrant is required under the act; however the aforementioned Telecommunications Act 1997 obligates the service providers to provide interception capability and assist Law Enforcement Agencies (LEA) with interception (Privacy International, 2004). More recently the Telecommunications (Interception and Access) Bill allows warrantless access to telecommunications data that does not include content. Location of a mobile phone user is not considered content, which conveniently enables surveillance of individuals with no judicial oversight.

In summary, there is no specific legislation in Australia regulating location information. In jurisdictions where privacy statutes exist, location information may still fall under information privacy principles; however, the complex nature of space and time, and the ability to process this information to generate new information has to be understood by the legal fraternity.
3. Location Privacy Concepts

Table 3.2: Summary of NPPs.

<table>
<thead>
<tr>
<th>Transport Application</th>
<th>Primary Data Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1 - Collection</td>
<td>describes what an organisation should do when collecting personal information. This includes rules about what information they collect, collecting information about a person from someone else and, generally, what information they should give about the collection.</td>
</tr>
<tr>
<td>Principle 2 - Use and disclosure</td>
<td>outlines how organisations can use and disclose personal information. An organisation does not always need consent to use and disclose information if they meet other conditions. There are special rules about direct marketing.</td>
</tr>
<tr>
<td>Principle 3 - Data quality</td>
<td>says that an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.</td>
</tr>
<tr>
<td>Principle 4 - Data security</td>
<td>sets the standards that organisations must meet for the security of personal information.</td>
</tr>
<tr>
<td>Principle 5 - Openness</td>
<td>requires organisations to be open about their privacy policy. Organisations must give certain information about the way they handle personal information in their organisation if asked.</td>
</tr>
<tr>
<td>Principle 6 - Access and correction</td>
<td>gives a general right of access to personal information, and the right to have that information corrected, if it is inaccurate, incomplete or out of date.</td>
</tr>
<tr>
<td>Principle 7 - Identifiers</td>
<td>says that generally, Commonwealth government identifiers (such as the Medicare number or the Veterans Affairs number) can only be used for the purposes for which they were issued.</td>
</tr>
<tr>
<td>Principle 8 - Anonymity</td>
<td>where possible, organisations must give one the opportunity to do business with them without identifying oneself.</td>
</tr>
<tr>
<td>Principle 9 - Transfer data flows</td>
<td>outlines privacy protections that apply to the transfer of personal information out of Australia.</td>
</tr>
<tr>
<td>Principle 10 - Sensitive information</td>
<td>requires your consent when an organisation collects sensitive information about you such as health information, or information about your racial or ethnic background, or criminal record. Sensitive information is a subset of personal information and special protection applies to this information.</td>
</tr>
</tbody>
</table>
3. Location Privacy Concepts

Other Jurisdictions

In the United States, common law gives rise to four generally recognised privacy torts: (1) intrusion upon a person's seclusion; (2) public disclosure of private facts; (3) publicity in a false light; (4) misappropriation of one's likeness. However, the public disclosure tort is not available when the event takes place in public. Constitutional protections for privacy, derived from the Fourth Amendment, restrict government intrusion into personal life through searches of persons, personal space, and information. The Wireless Communications & Public Safety Act of 1999 makes specific provision for 'wireless location information privacy' regarding a telecommunication carrier's use and disclosure of customer proprietary network information (CPNI). Location forms one of the sensitive categories of data that require protection by carriers: apart from emergencies they are forbidden from accessing, using or disclosing wireless location information 'without the express prior authorization of the customer' (Privacy International, 2004).

In the European Union, the Directive on Privacy and Electronic Communications (2002/58/EC) issued in 2002 establishes 'technology-neutral' legal standards for privacy protection in the processing of personal data for all electronic communications. Article 9 of the Directive unambiguously requires informed opt-in consent for the provision of telecommunications services based on the use of location information. Subscribers must be able, without charge, to withdraw their consent for the collection or processing of their location information at any time. Article 9 leaves it to member countries to decide what constitutes consent and how it is to be obtained and withdrawn (Ackerman & Miki, 2003). The UK Data Protection legislation does not consider location information as sensitive information. There are some limits on disclosure under telecommunications legislation.

UK data protection legislation does not privilege 'location' as one of the categories of 'sensitive' information (ie data relating to racial/ethnic origin, political
opinions, religious or other beliefs, trade union membership, health, sex life or criminal convictions). There are some limits on disclosure under telecommunications legislation (Caslon Analytics, 2008).

### 3.6.2 Case Law

In many instances case law has interpreted location privacy rights by examining the intrusion of technology into the private sphere, technologically enhanced government searches, and the use of mobile tracking devices and telecommunications information to derive the whereabouts of an individual. In US contexts, the fourth amendment test is not applicable to what is knowingly disclosed in public; however, courts have ruled that the use of technologies not available to the general public can violate privacy expectations. On the other hand, courts have shown a willingness to allow LEA to use technologically-enhanced vision for searches, flying over fenced backyards, industrial plants and greenhouses, suggesting that there is no reasonable expectation of privacy in open fields (Kisselburgh, 2006). In summary, legal protection for location privacy is not consistent across jurisdictions.

In *Katz v. United States*, a man used a glass-enclosed public telephone booth, which was wiretapped by the Federal Bureau of Investigation (FBI), for making gambling related calls in violation of a federal law preventing the use of *wire communication facilities* for transmitting a wager. The FBI presented the recorded phone call as evidence, but the Supreme court considered this evidence inadmissible on the grounds that the wiretap was a violation of the privacy which the man should have assumed attached to his conversations. Even though the conversation took place in public, this was considered search and seizure within the meanings of the Fourth Amendment. The court established a *reasonable expectation of privacy* test, which consisted of two standards. First, a person must have an actual expectation of privacy in a certain situation. Second, society
must be prepared to recognise this expectation as reasonable (Kisselburgh, 2006).

In 2001, two defendants were identified by LEA as active drug traffickers. Court orders were obtained to intercept communications, toll records, and other information relevant to the investigation. Though visual surveillance was conducted, it was not always possible to keep the defendants in sight. Rather than waiting for the defendants to place calls and then to access the provider’s records to gain knowledge about their whereabouts, the detectives dialled the defendants' cell phone number without allowing it to ring. This information was used to determine which transmission towers were being used by the defendant’s cell phone. This location information was then used to reestablish visual surveillance of the defendants. The court rejected the defendants’ appeal that the use of this information turned their cell phones into tracking devices by arguing that these were electronic signals rather than wire or oral. The court concluded that the use of tracking units does not bar evidence obtained through the use of such devices (Kisselburgh, 2006).

In April 2005, the Bundesverfassungsgericht (German Federal Constitutional Court) ruled that regulations in the Strafprozessordnung (StPO Code of Criminal Procedure) concerning police use of GPS as a surveillance tool did not violate the German constitution, as long as this technology was not used in conjunction with other surveillance methods which could lead to the construction of a personality profile of the subject (Jacoby, 2005).

This ruling was in response to a complaint in which the claimant alleged that the use of GPS coupled with other observation methods was cumulatively unconstitutional under Article 1 & 2 of the German Grundgesetz (Constitution), where these articles provide the following protections (Jacoby, 2005).

1. Article 1 (1): Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority (Jacoby, 2005).

2. Article 2 (1): Every person shall have the right to free development of
his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law (Jacoby, 2005).

Although the court noted that the use of GPS technology was an attack on the suspect’s personality rights, the extent and intensity of this invasion was not at a level that violated human dignity or the core sphere of privacy. The right to personality, according to German law is not an absolute right, unlike the human dignity clause.

The court stressed that the use of GPS technology was limited to revealing the person’s location and the time spent at a given location. The court, however, noted that total surveillance (multiple simultaneous observations) leading to the construction of a personality profile was unconstitutional.

Further, the court described the home as the last refuge for the development of one’s personality, and the right to retreat into one’s home was absolute. Personal communication receives greater protection from the law than one’s whereabouts. Given the rapid development of location technologies, it is unlikely that the court’s decision is far-reaching. Mobile phones with AGPS and technologies such as Google Latitude, which create geo-coded databases of cell-tower signals and Wi-Fi signals, are now able to accurately locate individuals in most terrains, even indoors or in the urban canyon (Google Latitude, 2009). Regardless of whether the person is travelling in a car, train or on foot, a personality profile could be constructed.
3. Location Privacy Concepts

3.7 Technical Mechanisms for Privacy Protection

3.7.1 Policy-based & Rule-based protections

If the growth in telematics services proceeds as predicted, then it will be difficult for a member of the public to keep track of all details about themselves when mobile. Secondly, constant explicit consent requirements could become a source of driver distraction. Hence an analogy can be drawn from the internet, where the Platform for Privacy Preferences (P3P) is used to manage web server privacy policies in Extensible Markup Language (XML) machine readable format. Typically these operate by comparing user profile rules of a web client with the rules on a particular web server. Such is the importance of location privacy that there are already efforts to extend the P3P for location rules (Morris, 2002). This means that rules like ‘Allow Alice to access my location on a weekday’ can be created.

Duri et al. (2002) have proposed an end-to-end framework based on a similar principle that provides both security and privacy within the telematics environment. However, there is one issue with this implementation. Since the policies serve as a mutual contract, the driver has to trust the organization to abide by the policies.

The Internet Engineering Task Force (IETF), the standards body responsible for developing internet standards, has also realized the importance of location privacy. It has proposed the Geographical Location/Privacy Charter, referred to simply as geopriv. This standard seeks to preserve the location privacy of mobile internet hosts (IETF, 2006).

Synnes, Nord, et Parnes (2003) have implemented secure location privacy, using a similar approach of using rules to implement policies. In the near future it is not hard to imagine automobiles having Internet Protocol (IP) addresses...
and ultimately using the geopriv solution to implement privacy policies.

3.7.2 Decoupling Identity & Location

A vehicle can be uniquely identified when it communicates with a particular telematics provider. In the approach of identity and location decoupling, location information could be removed from the identifying information at the time of data retention. This could be regulated through policy, and laws such as those discussed above. Herborn, Boreli, et Seneviratne (2005) have studied this concept in pervasive computing networks. They argue that decoupling these data from each other would have more benefits. Name hijacking would simply not be possible. The issue here is that for decoupling the identity and other data to work, a robust scheme to resolve naming would be required. This, however, is still an open research issue.

3.7.3 Anonymous Access

Researchers in the field of LBS have looked at anonymous solutions to location privacy. The basic idea here is to access the services anonymously. Unfortunately this cannot be regarded as a complete solution, given the inference capabilities of GIS and advanced surveillance techniques, as discussed already (Gruteser & Hoh, 2005). An adversary can apply data-matching techniques to independent samples of anonymous data collected, and map them on predictable paths such as roads, and infer the identity of an individual based on where one is.

Drawing on techniques used by census boards and electoral commissions to obscure data, so that individuals are not identified, another methodology similar to anonymous access has been proposed. It is called k-anonymous access. This means that when the location information of a subject is requested, it will only be responded to if there are $k$ other nodes present in the vicinity (Gruteser & Grunwald, 2003). This approach can give good protection against privacy
attacks if the value of $k$ is set to a high number; however this would affect the quality of service of LBS. In this approach, $k$ is a variable that could only be altered globally. A second approach deals with $k$ on a per node basis. This means that each user can specify their privacy variable (Gedik & Liu, 2005). This approach appears to more realistically simulate user privacy preferences in the real world.

Apart from being identified through map-matching techniques, there is one additional problem that can affect the correct operation of telematics services using anonymous techniques. Existing approaches discussed here are aimed at solving the location privacy problem in the context of LBS. Telematics can be considered to be a special case of LBS, however, as it needs a totally different mindset for addressing privacy problems of the mobile public, mainly because of differences such as higher average speeds, predictable paths, and the magnitude of the number of users.

### 3.7.4 Obfuscation

The term obfuscation means the process of confusing or obscuring. It has been identified as one possible approach to protecting location privacy in location-aware computing (Duckham & Kulik, 2005). This deliberate degradation of location information is performed by the individual through deciding which service would require what granularity of information, often referred to as the need to know principle.

Snekkenes (2001) constructed rules for implementing privacy policies using this principle. He emphasized that different services require different resolutions, or accuracy, of location information. The advantage of obfuscation over anonymity is that it allows authentication and customization of the services. However, it still is not the ideal remedy when high accuracy of reported location, instead of deliberate degradation, is required.
3.7.5 Privacy-aware designs

While the defense methods discussed above propose measures for limiting disclosure of location information, others have sought to understand privacy aware designs. The success of future LBS and telematics systems depends on designing systems with privacy in mind, not just having it as an afterthought. Langheinrich (2005) discusses the need for anonymous location infrastructures and transparency protocols allowing customers to understand and track how their data is collected and used.

Kobsa et Teltzrow (2006) argue that clearly explaining privacy policies at subscription would encourage users to disclose information and create a sense of trust. They conducted experiments to prove this, comparing their privacy friendly systems to the traditional data collection systems.

Other examples of privacy aware designs include work by Coroama et Langheinrich (2006), where they implemented a GPS based PAYD insurance system depicting real time risk assessment of actual road conditions and preserving the privacy of owners. There is periodic transmission of aggregated information to the insurance provider for bill generation.

3.8 Research Gap- Privacy-aware Mobility Pricing

The success of mobility pricing is largely dependent on how location privacy issues are handled. Privacy-aware designs could help in ameliorating these concerns. The review of the literature has identified the following potential research gaps.

1. The legal and ethical implications of the collection, use and retention, both in real-time and retrospectively, have not been fully understood by the law and by society.
3. Location Privacy Concepts

2. The most important stakeholder, the motorist, is not aware of the capabilities of location and tracking, and its implication for their autonomy and privacy.

3. The opinion of motorists or users has not directly been sought when it comes to designing privacy enhancing technologies. Opting in for the provision of data is not a binary operation, where the persona opts-in to provide all information, or provides none and undergoes denial of service. Personal preferences are defined by context: an individual might have no problems in disclosing precise location information during office hours to his boss while at site, but may have objections in disclosing location after work hours.

4. Proposed pricing models that aim to convert manual processes to electronic counterparts have not covered all issues; for instance the anonymity that was an essential part of manual systems has simply vanished from electronic versions.

The main aim of this research has been to perform analysis of current mobility pricing solutions from legal and ethical standpoints and to identify what vulnerabilities exist in these systems. This analysis includes identifying whether it is appropriate to track the location of motorists at all times, or whether other alternatives could be devised that do not depend on continuous transmission of location information. Additionally, this research has aimed to study user perception when it comes to privacy-aware designs, pricing and location privacy. Finally the aim has been to use these analysis and user perception results as inputs into a privacy-enhancing technology framework without compromising on the benefits that telematics-enabled road-pricing offers. It is envisaged that a privacy-preserving technology solution which has taken both social and ethical issues on board would be highly acceptable to the community without disadvan-
3.9 Summary

Location privacy is a social, regulatory, policy and technology issue that has emerged with the appearance of location-awareness and the advent of location-based services for public safety and commercial purposes. The telematics-enabled vehicle is not only a mobile computing platform, it also stores information about the behaviour of the motorist which could possibly be used to incriminate them.

The advent of internet has raised privacy issues on a scale not witnessed before. Privacy in the online world can be considered differently to a 'traditional' notion of privacy. On the other hand, the threat posed to location privacy by convergent technologies concerns both the physical space and the cyber-space and needs different approaches for protection. It far outweighs the threats posed in the traditional or the online world. This chapter has reviewed the legal, social and technical mechanisms for privacy protection. None of these approaches provide a complete panacea for protecting privacy on roads. It seems likely that a combination of approaches is required, involving social research, legal instruments and privacy-aware technology solutions.

While telematics-driven road pricing promises a reduction in congestion, fairer charges and the reduction of environmental hazards, the challenging issue is to preserve location privacy while at the same time maximising the benefits of telematics services. The forthcoming chapters address possible solutions for a privacy-aware mobility pricing framework.
Chapter 4

Privacy Assessment of Two Mobility-Priced Applications

4.1 Introduction

This chapter examines two mobility pricing applications, namely ETC and PAYD, with regards to location privacy, and makes policy recommendations that could be useful in restoring anonymity in these applications. To develop these recommendations, a range of material has been examined, which includes case law, current regulations, and the privacy challenges presented by these applications. These privacy challenges are evaluated by employing an analysis framework that measures how invasive these applications are with respect to the privacy of motorists. This framework compares the non-electronic equivalent of the applications, evaluates the choice and consent available, identifies whether a system involves active surveillance or passive surveillance, compares the granularity of location information collected, and measures the degree of identifiability from the data collected. It is envisaged that the developed policy recommendations would be useful in providing a common approach to facilitating the development of strategies for privacy-aware mobility pricing.
4.2 Analysis Framework

The following are the components of the framework used to evaluate location privacy concerns in mobility-pricing.

4.2.1 Non-Electronic Equivalence Test

The non-electronic equivalence test compares the key differences between the traditional and electronic counterparts of mobility pricing. This test evaluates how and whether anonymity is preserved in an electronically priced system. By reverse engineering the functionality of electronic systems back to a manual equivalent, this test compares the amount of data gathered in a traditional system with the non-electronic version of an electronic system.

Traditional systems had human participants, where processing and distribution of information was limited by human capacities. It is unlikely that an observer is able to maintain complete surveillance of one or more vehicles at all times as there are natural barriers to physical surveillance (Nissenbaum, 2004).

An electronic system is usually designed by abstracting the participants and their actions in the non-electronic world. It is vital to understand that anonymity, which is an important aspect of the non-electronic world, has to be abstracted appropriately to have a true electronic conversion of a manually operated system or concept. By removing the technology aspects from the equation and critically analysing the non-electronic equivalent, the aim here is to identify potential implications of these systems to locational privacy.

4.2.2 Active vs. Passive Systems

Another important test applied in this analysis is to evaluate whether a technology is active, that is, whether it actively engages with the participant's requests, or is passive, that is, it passively generates responses based on the user's context,
which is location in this instance. Active vs. passive technologies have also been defined as push vs. pull, or proactive vs. reactive (Kuitjper, 2005; Raper, Gartner, & Rizos, 2007). Active services are explicitly invoked by the user and the location of the user is only registered at a particular event, whereas, in a passive system the location of the user undergoes continuous monitoring and tracking to identify events, and no explicit requests are made by the user of the service.

In the case of an active system, the user is generally aware that an event is registered on the basis of an action or the location (proximity-based actuation) of the user and this event registration may cause a behaviour modification on the user’s part if the user wants to avoid registration of that event. On the other hand, in the case of passive systems, there is implicit consent by the user to the registration of all events that take place in the life-cycle of the service. With the passage of time the user might become unaware of the presence of this system and would go about their daily business, thus losing control of the location information generated about them.

4.2.3 Identifiability

Current location-based systems appear to provide a clearer connection between an individual’s locational activity and identity. While some of the systems that record the position of the user also take note of the apparent identity (licence plate number) of the user, such as ANPR, speed cameras, red light cameras, CCTV and other systems may still infer identity from anonymous data, on the basis of the patterns of movements of the users. This test critiques the degree of identifiability of individuals that is available in these two mobility pricing applications.
4.2.4 Consent and Choice

This test consists of two parts. The first one, consent, assesses whether the user provides explicit consent in the disclosure of location information or whether there is implied consent with the use of the service. Choice refers to whether the user has the option of not taking up a particular pricing option and system. Would the user be disadvantaged if they did not enrol in the system?

4.2.5 Locational Granularity

Granularity refers to the degree of detail or precision contained in data. Granularity has several dimensions, including spatial granularity and temporal granularity. Spatial granularity refers to the size of a geographical cluster where an individual may be placed with a degree of certainty, whereas temporal granularity when used in conjunction with spatial granularity may reveal that at any time ‘t’ an individual was identified to be in a certain geographic cluster ‘c’. The smaller the cluster, the more granular is the spatial information. The granularity at which the individual expects the location data to be exposed may have an effect on privacy and location disclosure decisions. This test assesses the locational granularity of data collected in tolling and GPS-enabled insurance scenarios.

4.3 Case Study I: Electronic Toll Collection

4.3.1 Privacy Implications of Existing Tolling Practices

As discussed earlier in 2.5.1, ETC promises alleviation of congestion problems, reduction of toll management costs, and cash-free convenience for drivers. These conveniences, however, are at the cost of loss of anonymity of motorists. Contracts between motorists and ETC providers, in general, require the following
details before an E-Tag is issued.

- Driver's name
- Address
- Phone numbers
- Email address
- Fax number
- Bank account number
- Credit card details
- Drivers' licence number including the state and expiry date
- Vehicle's make, model, colour and year of manufacture.
- Vehicle's Number plate details, including the State/Territory and the number displayed on the vehicle's number plates

These E-Tags emit unique electro-magnetic signals when drivers pass toll gantries. On the basis of this unique identifier, the associated contract information is retrieved, and relevant toll charges are debited to the account. Transactional data includes detailed information such as date and time of passage, photographic images of the vehicle at the time of passing through the toll gantry, the location of the toll gantry and the amount of the toll fee, all of which is recorded in an electronic storage repository (a database) for invoice generation purposes and possible dispute resolution. Comprehensive information about the motorist's movement is retained for as long as seven years (ROAM E-TAG, 2007). Figure 4.1 summarises the transactional and registration data collection for ETC.
The identifiable nature of these transactions raises issues of personal autonomy and privacy for motorists. While the anonymity of motorists can be maintained on toll roads where cash payment booths are operated in tandem with electronic toll lanes, it appears that future tolling systems will be exclusively electronic, and will not offer the choice of anonymous travel to motorists. Retention of data means that detailed travel profiles of motorists could be erected to make inferences about their movements. Recent developments in transport technology for the purpose of enforcement, policing, road safety and road pricing, involve a systematic request for the road-users' identity. This gradual shift has enabled mass surveillance which is contrary to community expectations.
4.3.2 Unique Identifiers

With electronic financial transactions, the account to be debited must be uniquely identified. For ETC, this unique identification is achieved by assigning the RFID tag to emit a unique identifier at toll gantries, which is then matched against an account previously set up by the tag user and the toll provider. The toll provider is not interested in which particular vehicle was granted passage, as long as the correct toll fee is charged. However, in order to electronically charge payments, this approach has become an implicit standard.

4.3.3 Extended Data Retention

ETC operations result in transactional data which is stored for the purpose of invoice generation. The data may be stored for a period of up to seven years, even if a patron terminates a contract before that time (ROAM E-TAG, 2007). While the requirement for data retention may be purely legal or tax-related, the temptation to use it for secondary purposes can be too great to resist, and seven years is sufficient time to enable 'function creep'. Holtzman (2006) describes seven sins of privacy. Among them is the 'sin of latency', which is prolonged retention of data. He argues that data should never be kept longer than needed for its original purpose. In tolling contexts, this means that once a bill has been paid, data related to that transaction, or at least, identification information including the location where the toll event occurred, should be purged.

Current retention policies give rise to three major issues. First there is 'unsolicited profiling', where long term collection of transaction data may be used to infer driver behaviour. This data can be mined using data-mining techniques to create profiles of patrons which can be sold to other agencies such as insurance companies. The privacy policy of one toll provider in Australia (Connect East, 2008) describes that the collected profile data include

- Records of journey itineraries and patterns.
• Patterns of regular passages of the vehicle past a particular ETC point.

• (Spatio-temporal) pattern irregularities.

While privacy policies can often use blanket terms to cover these scenarios, consumers should be able to question the exact need for the use of this information if the primary purpose of collection was payment processing. The second issue is ‘unsolicited tracking’, which means that real-time location and heading of a vehicle can be identified and may be used as a surveillance device by totalitarian governments. The issue of profiling and tracking may be further intensified by a third problem known as ‘data-merging’. It is possible to use the unique identifier obtained from the toll tag to infer the identity of the patron, and to use this identity to query disparate databases and extract volumes of information about them.

Extended data retention carries significant risks for all stakeholders since the possibility of data compromise cannot be ruled out, whether this is performed by a legitimate user for illegitimate uses, or by illegitimate hackers with the aim of sifting information about motorists. These scenarios can cause abstract losses e.g. reputation and defamation, and have financial implications e.g. credit card theft and government fines for associated data breaches.

One such example from the tolling industry occurred a few years ago when an ex-employee of an ETC provider in Australia admitted in court to passing credit card details of about 8000 customers to cyber-thieves for their shopping sprees (HCi, 2007). A review of the privacy policies of the company by the Office of The Federal Privacy Commissioner (2002) revealed that additional steps were required to reduce the risk of privacy breaches. The report also acknowledged that addressing those privacy risks does not necessarily prevent similar future breaches. Neither the law nor technology can prevent these events when it comes to human motivation. In summary, services which deliberately ignore privacy-respecting implementations and collect, store and process personally identifiable
information should be prepared for the hidden costs, in the form of risks associated with data breaches.

### 4.3.4 Secondary uses

Function creep means that information collected for a particular purpose also ends up serving other unrelated purposes. An interesting secondary application based on tolls has been implemented in Texas, US, to predict how congested current roads are. A third-party application mimics the communication exchange that a toll booth would demand from a transponder, and exploits this vulnerability to build a system of RFID readers installed on various sections of the highway.

The results are then used to calculate the average traffic speed on each stretch of road, and are made available in near real-time on a website for motorists to plan their journeys (Houston Transtar, 2008) as shown in Figure 4.2. While this application might be a blessing for motorists who can get information about road conditions before setting out, it can also become a serious threat as it exposes a vulnerability which could be abused by individuals with malicious intent.

Related examples of tolls that go beyond the realm of simple toll collection include payment of parking fees at Albany, Newark and John F Kennedy Airports in the US (The New York Times, 2000) and use of the toll tag for payment of meals at select drive-through McDonald’s restaurants (USA Today, 2001).

Another potential concern is the legitimate use of toll information by law-enforcement agencies conducting criminal investigations. In the United States, both criminal and civil court cases are being won and lost on the basis of toll records. Toll records helped convict a New Jersey nurse accused of murdering her husband. Her toll records were used to reconstruct her movement which showed she was near the Chesapeake Bay, Maryland, US on the night of the murder. Three matching suitcases with the remains of her spouse were later recovered.
from the Bay, which ultimately lead to her conviction (Ryan, 2007). In another incident, 30 New York police detectives were reportedly re-assigned after their toll records suggested they were making false overtime claims (Renegar, Michael, & Michael, 2008).

While use of toll data may be acceptable in criminal cases of the severest kind, toll companies are actively being subpoenaed in civil matters such as divorce proceedings to prove adultery. A privacy rights advocate has noted that people who want to protect their privacy should not use electronic toll systems (Newmarker, 2007). This advice may be appropriate on roads where cash booths are operating in tandem with electronic tolling lanes; however, electronic toll col-
4. Privacy Assessment of Two Mobility-Priced Applications

MobileCloak
Interior: 4 1/2"(w) x 7"(h)

Figure 4.3: mcloak pouch used for shielding toll tag signals. Source (Mobile Cloak, 2009)

lection is becoming de facto standard for toll collections, and it appears that in the next few years human-operated toll booths will become nonexistent.

4.3.5 Security Vulnerabilities

As discussed in Section 4.3.4, the Houston real-time traffic map system mimics the communication protocol between the toll gantry and transponder to ascertain traffic congestion. This exposes a vulnerability in the design of current transponders which lack encryption. A person with the right tag reader walking through a parking lot can steal the unique radio-identification signal from transponders fitted to the windshields and clone new tags and use them with the victim footing the bill for their use of tolls (Mills, 2008).

Recognising this issue, security experts have developed a simple yet effective solution. They have designed a special pouch for the wireless tags, which shields the electromagnetic waves from leaving or entering the pouch (Mobile Cloak, 2009). Users can put their toll tags in such a pouch, preventing anybody from
scanning their tags, and are advised to take the tag out only when approaching a toll gantry, thus limiting the vulnerability. These 'incloak' or mobile cloak pouches (as illustrated in Figure 4.3) are available for purchase online. These pouches reduce the signal attenuation to 80 dB which is equivalent to 0.00000001 of input signals in the range of 10MHz to 20GHz (which covers a range of wireless devices, including WiFi, mobile phones, GPS, Toll Tags).

4.3.6 Legislative Instruments

It has been discussed in Chapter 3 that in the year 2000 the privacy legislation in Australia was extended to cover private sector organisations. The NPPs are the baseline privacy standard that most private sector organisations have to comply with in relation to the personal information they hold. Principal 8, anonymity, is highly relevant to mobility pricing. This principle states that,

"Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation." (National Privacy Principles, 2001)

4.3.7 Standard for Privacy of Toll Collection

Standards Australia is recognised by the Government as Australia’s peak standards body and develops standards of public benefit and national interest. The Committee IT/23, Transport Information and Control Systems within Standards Australia, developed a code for the handling of personal data of motorists by electronic toll operators (Standards Australia, 2000). The document states that it is technically feasible to design anonymous toll collection systems. While ETC is based on technology by which unique identifiers are assigned to the tags, these identifiers should not necessarily be related to a vehicle’s identity. The document even suggests using smart-card enabled tags that can provide the same functionality without the need for storing identifying data.
4. Privacy Assessment of Two Mobility-Priced Applications

This standard also provides detailed guidelines for the implementation of anonymous operations. Recommendation 4 from the standard states that the operator should provide customers with the option of anonymous operation, either on a permanent or a casual basis, and specific advice should be provided about the implementation of such operation (Standards Australia, 2000)[p. 13].

4.3.8 Disregard of NPP 8 and Privacy Standard

The privacy policy of at least one toll operator in Australia claims compliance with the NPPs and AS 4721 (CrossCity, 2007) but they do not support anonymous operation, which is in contradiction to NPP 8 and Recommendation 4 of AS 4721. The argument given by the toll operators is that collection of identifying information of motorists is 'necessary' for the operation of tolling, thus providing ‘acNPP 1.1 (collection limitation principle, discussed in Chapter 3) as their justification for collecting this information.

The ongoing need for NPP 8 to be incorporated in systems design also exposes a weakness of the current complaints-based enforcement model. Complaints targeting a breach of NPP 8 would probably be knocked back, because toll operators can legitimately argue that it is ‘impracticable’ to implement anonymous options in already established systems. This leads to the importance of effectively enforcing these principles by a proactive regulator who is prepared to intercept organisations designing new systems, and demand from them how they plan to implement the anonymity principle.

Unfortunately, in Australia regulators have only been able to acknowledge that toll data can be a potential treasure trove for invading motorists’ privacy (Office of the Victorian Privacy Commissioner, 2004 : Privacy NSW, 2004 : Crompton, 2004 : Curtis, 2006), rather than tackling the core issue by engaging with toll providers and enforcing the privacy principles, especially that of anonymity. Moreover, recent communiqués from privacy regulators represent
a shift to acceptance of electronic tolls as the standard way of collecting toll charges. The argument provided is that anonymous travel on roads is less important than other competing public interests such as efficiency, flourishing commerce, public safety and environmental concerns (Office of the Privacy Commissioner, 2008; Office of the Victorian Privacy Commissioner, 2008; Privacy NSW, 2008).

While toll road operators have an obligation under Commonwealth Privacy Laws to provide anonymous payment options, another legal gray-zone is that toll roads built in public-private partnership. It is unclear whether federal or state privacy laws govern their operations. Under Section 7B of the Privacy Act, organisations acting under state contracts are exempt from the Privacy Act, and would be covered by the state or territory’s privacy legislation (The Privacy Act 1988, 2009).

For instance, the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP), applicable to state authorities within NSW, does not include an anonymity principle. This vulnerability has been exploited by toll providers arguing that they are not legally required to implement the anonymity principle since they are under a NSW state contract with regards to the toll road operation. However, recently the ALRC has recommended inclusion of Uniform Privacy Principles across privacy laws in Australia. If this recommendation is implemented in state and federal privacy laws, then it is possible that public-private state contracts would have to provide anonymous payment options (Australian Law Reform Commission, 2007, 2008).

4.3.9 Review of Toll Applications

Dynicash in Japan and the Netherlands

Dynicash was the first anonymous toll collection system installed in the Netherlands and Japan. This system worked on the principles of cryptographic blind
digital signatures to create digital cash (Chaum, 1989; Tetsusaki, 1994).

A smart card-enabled transponder using digital cash (Chaum, Fiat, & Naor, 1990) was used for tolls, which contained electronic tokens equivalent to cash. When a vehicle fitted with such a device came in proximity of a toll booth, a communication protocol took place between the road-side equipment RSE and the on-board unit OBE. After the verification process the OBE sent a digital cheque to the RSE, which the RSE could verify that it came from the bank (using the bank's public key signature). The toll company then sent this cheque to its collecting operator's bank. This smart card also carried indisputable proof of payment for the patrons' protection and records.

This system provided the desired functionality by balancing the privacy needs of the motorist, who could still travel the roads anonymously and those of the operators by providing the correct amount of toll fees to toll collection authorities without them requiring to maintain large databases of motorists' movements. Unfortunately, this system did not progress well. Some observations that can be made about this system are that it used pre-paid tags, where patrons may have been reluctant to invest in a service which they planned to use only occasionally and that it was probably ahead of its time.

Melbourne's City Link Project

The Melbourne City Link Project in Victoria, Australia, built between 1996 and 2000, was one of the world's first and largest fully electronic tolling systems. There were concerns by the public about cashless tolling, so anonymous accounts were offered by Transurban, the company which manages the City Link. A document obtained from the Victorian Parliament's website relating to anonymous toll is cited below:

"Transurban proposes to offer an anonymous account under which owners may avoid disclosing personal or vehicle registration details."
4. Privacy Assessment of Two Mobility-Priced Applications

Special commercial conditions apply to such accounts.” (Victorian Parliament, 1998)

A review of Transurban’s privacy code (MG & Daley, 2002; Ogden, 2001) provided finer details of this anonymous account. Prospective clients interested in using the tolled roads without divulging personal information had the option of paying a $50 security deposit to get an ‘E-Tag’. The deposit was refundable if the E-Tag was returned at a future date. The clients were required to physically receive their transponders from an office. Additionally, clients were responsible for maintaining sufficient credit in their anonymous account, and would lose anonymity and receive legal notices if the vehicle passed the toll booth with a zero credit or the transponder malfunctioned. It is unclear whether the toll provider actually provided anonymous accounts, as a recent search on both City Link and Transurban’s websites for the word ‘anonymous’ returned no responses.

Highway 407, Toronto, Canada

The 407 Express Toll Route (ETR) is a fully electronic toll road that, theoretically, offered anonymous transponder accounts, similar to the City Link Project. The privacy provisions for anonymous accounts were developed in consultation with the Information and Privacy Commissioner (IPC) of Canada. The IPC even made available a public awareness document explaining how one could travel the 407 anonymously (Cavoukian, 1998). Thompson et Kerr (2005) have shown that despite clear directions on how to achieve anonymity by the IPC, the anonymous option described above did not exist on the toll authority’s website. The number of anonymous accounts, according to the toll providers, was twenty one, which meant that there were only four anonymous transponders in a pool of more than six million transponders. Perhaps the administrative burdens, similar to those in the City Link project, of visiting a location during business hours, and still providing some form of personal information (credit card details kept on file,
in this case) were not worthwhile for individuals to protect the privacy of their movements.

**Hong Kong’s Autotoll**

S. Garfinkel (1996) reports that the Hong Kong government in the mid 1980s introduced a sophisticated electronic road pricing system to tackle congestion and pollution issues. Shortly after its deployment, questions were raised about the ability of this system to track movements. Drivers began receiving statements about where and when they were charged a toll fee. Citizens of Hong Kong expressed concern about the use of this data for political reasons, especially in the post 1997 era when China was to take back control of Hong Kong. As a result of these protests, this system had to be withdrawn (Hau, 1990), which is an interesting example of how political and social factors can affect electronic pricing.

A more recent review of electronic tolling in Hong Kong reveals that there is an efficient and extensive electronic road pricing system known as Autotoll. The toll system is pre-paid, where payments are deducted from a pre-paid account but still all transaction details (date, time, location, etc.) are stored for access to subscribers. Additional investigation has shown that the same company even provides auto insurance policies. It can only be left to the imagination how the data collected from these toll transactions could be improving actuarial models and insurance premiums.

### 4.3.10 Survey Research

In order to seek community opinion about toll-collection related privacy issues, various surveys have been conducted. The Royal Automobile Club of Victoria (RACV) undertook research in 1998 to gauge respondents’ views in the context of the Melbourne City Link project (Ogden, 2001). Results of this survey show that
28% of the respondents expressed concern about their movements being stored electronically, with 73% of this group citing invasion of privacy as the reason for concern. When asked if the respondents would be interested in operating anonymous accounts, 43% expressed interest in such a facility and 11% indicated that they would prefer to travel anonymously at any cost.

Another study conducted by the University of California at Berkeley for the Department of Transportation (DoT) in the United States also identified privacy issues as a concern for users (Yim, 1991). The respondents were asked about cashless payments and the potential to trace vehicle location. Of those respondents who used tag-based payments, 16% expressed concerns about privacy issues.

These statistics indicate that there is a significant proportion of the population who are concerned about privacy and are willing to forego some of the benefits technology offers in order to protect their freedom of movement.

4.3.11 Analysis Framework

With an in-depth study of the toll related privacy issues described in sections 4.3.1 -4.3.10, a critical analysis, using the proposed framework, has been performed on these issues in the following sub-sections.

Non-Electronic Equivalence Test

It appears that the non-electronic equivalent of current electronic toll practices would be an employee of the toll company present in one of the toll booths at the toll plaza who demands the driver’s unique identification details and takes the driver’s toll. Additionally, the toll attendant would record the time, date and location where the vehicle crossed the toll gantry. The toll attendant would also note down the registration details of the vehicle taking a picture of the rear licence plates. Records collected by all attendants would then be consolidated.
in one massive database and retained indefinitely. There is a stark difference between this collection procedure and standard manually operated toll booths.

The non-electronic equivalent of the Houston Transtar system would be a collection of persons equipped with tag-readers, strategically placed in different locations on the highway, who capture the vehicle’s unique identifier and count the vehicles passing a point in a particular period to evaluate the average speed at that point, and possibly to note down the vehicle’s unique identification signal emitted by the transponder. All this information would then be transmitted to a central repository for visualisation of the congestion map.

**Active vs. Passive Systems**

Drivers approaching an electronic toll gantry are generally aware of the operation of electronic toll booths, via the visual signs informing them of which particular lanes are electronic and which are not, in addition to the ‘beep’ sound which emanates from the toll tag when the vehicle passes the toll plaza. This is an active interaction between the toll gantry and the transponder fitted in the vehicle.

However, this very interaction may become a passive one in the case of the Houston Transtar system, which uses the same toll infrastructure without the knowledge and possibly ‘explicit’ consent of the motorist. The driver is not aware of which toll readers are interacting with their transponder fitted in the vehicle, as they are not informed of the interaction either via visible signs or auditory beeps. In the case of toll operations, the beep informs the motorist of a successful toll transaction, and would probably become a source of driver distraction if they were to beep every time a map tag sensed a presence. This is precisely the issue: that the user is not aware that a tag reader has sensed their transponder’s presence and noted down its unique RFID signal. This potentially enables surveillance of the motorists’ movements by an interested third-party who has access to a toll-tag reader and wants to track a particular motorist or
many motorists. A possible countermeasure to avoid this passive surveillance has been discussed in Section 4.3.5 namely the use of an electromagnetic-signal shielding pouch.

**Identifiability**

With toll transactions every tag emits a unique signal which is used by the electronic toll infrastructure to retrieve the associated toll account and make debits from it for the toll charges. If the toll tag fails to beep, a photograph of the rear licence plate provides registration details via the ANPR system. The tag identification number or vehicle registration number can be used to pull up the account details which can identify the owner of the vehicle who may be the person who mostly drives the vehicle. Regardless of the distinction between the person driving the vehicle and the person who owns the vehicle, the identifiability aspects of electronic toll tags is strong, because they can be used to reasonably ascertain the identity of a living person and their vehicle’s presence at a particular toll gantry location at a particular time. This information falls under the definition of private information as per the discussion in Chapter 3.

**Consent and Choice**

A motorist provides consent to the use of his/her personal information by agreeing to the terms and conditions of the contract. The terms might cover the use of personal information for legitimate functions and activities including calculating and charging tolls, operating and maintaining the account, audit reporting and fulfilling legal requirements. The motorist may decline to be contacted for other products or services. In short, the toll authorities have the motorist’s consent to the use of their private location information for the primary purpose of generation of toll invoices.

In the case of secondary uses, such as the generation of congestion maps by a
third-party, no consent is obtained from the motorist to have their tags sensed. This method simply exploits the toll collection protocol by broadcasting signals that a toll gantry would have used to demand credentials from the toll tag. Once it receives these credentials it simply withdraws to engage in the protocol since all it requires for map generation is to sense that a vehicle has passed.

In Australia, ETC has been around for over ten years now, but motorists have had been able to choose whether or not to trade a little privacy for the convenience of a faster trip. However, the gradual phasing out of cash booths on Sydney toll roads, and no offer of anonymous electronic accounts means that a motorist does not have the option of anonymous travel without being disadvantaged in terms of time travelled by taking alternate routes they must withdraw their expectation of personal privacy. Sometimes taking an alternate route might not be an option, when the toll road is the only way of getting from point A to point B in a reasonable amount of time.

The choice of not interacting with a tag reader is only available by putting the E-Tag in an electromagnetic shielding pouch. Otherwise, the tag readers are free to demand the tag’s credentials in the current un-encrypted architecture which does not support mutual authentication.

<table>
<thead>
<tr>
<th>Toll Road</th>
<th>Number of toll gantries</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$ (Eastern Distributor)</td>
<td>3</td>
</tr>
<tr>
<td>$M_2$ (Hills Motorway)</td>
<td>6</td>
</tr>
<tr>
<td>$M_4$ (Western Motorway)</td>
<td>1</td>
</tr>
<tr>
<td>$M_5$ (South Western Motorway)</td>
<td>4</td>
</tr>
<tr>
<td>$M_7$ (Westlink)</td>
<td>48</td>
</tr>
<tr>
<td>Lane Cove Tunnel, including Falcon Street</td>
<td>6</td>
</tr>
<tr>
<td>Sydney Harbour Bridge &amp; Tunnel</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Toll Gantries</strong></td>
<td>102</td>
</tr>
</tbody>
</table>
Locational Granularity

The granularity or the resolution at which location information is available for motorists' use of electronic tolls largely depends on the density of the tolling network. A toll event identifies that a particular vehicle was last seen by the system at a particular location, traveling in a particular direction at a particular time. Thus if a motorist sets out for work early in the morning and uses the toll road to reach their workplace, this event would be registered. If the motorist has to leave from the workplace a few times for errands, and does not employ the use of toll roads, those movements are not recorded.

To get a rough idea of the smallest spatial cluster that a motorist could be placed into, the administrative boundaries spatial dataset obtained from Public Sector Mapping Agencies (PSMA) was loaded into a Spatial Database, Oracle 10G in this case (PSMA, 2009). A spatial Structured Query Language (SQL) query was run that returned the total area of all Local Government Area (LGA)s in Sydney to be roughly 12144.6 sq km. If this value is divided by the total number of toll booths operating on the 9 tolled roads in Sydney, the total number of toll plazas amounts to 102, as summarised in Table 4.1.

The resolution of a cluster obtained by diving the area of metropolitan Sydney by the total number of toll gantries is approximately, 119.06 sq km. This means that the location granularity of tolls is not alarming at this stage. However, if third party tag-readers become pervasive, the spatial resolution as well as the locational granularity would become high since it would represent a shift from proximity-based observable surveillance to a sophisticated and ubiquitous network of omnipresent surveillance.

4.3.12 Policy Recommendations

The results of the analysis are summarised in Table 4.2. The following are some recommendations that are made in the light of this analysis.
Table 4.2: Summary of the analysis framework results for ETC.

<table>
<thead>
<tr>
<th>Test</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-electronic equivalence test</td>
<td>Non-electronic equivalent of electronic tolls is a toll attendant recording the unique signal emanating from the vehicle's transponder, along with the vehicle's registration details, the vehicle's bearing, the toll location and time, and a photograph of the vehicle's rear licence plates.</td>
</tr>
<tr>
<td>Active vs. Passive system test</td>
<td>Mostly an active system, however with pervasive tag-readers (not primarily for toll collection), it has the potential to become a pervasive system.</td>
</tr>
<tr>
<td>Identifiability test</td>
<td>There appears to be a strong correlation between a toll transponder's unique identity and a vehicle's owner, hence the motorist is highly identifiable.</td>
</tr>
<tr>
<td>Consent &amp; Choice test</td>
<td>There is express consent in the use of electronic toll plazas. Consent is not obtained by a third-party just probing the presence of a transponder. Motorists are denied the choice to remain anonymous if all toll roads are electronic, with no anonymous account options available.</td>
</tr>
<tr>
<td>Locational granularity test in Sydney</td>
<td>Current locational granularity is not alarming. For any E-Tag vehicle the cluster size for Sydney is 119.06 sq kms. This might increase if tag-readers become pervasive.</td>
</tr>
</tbody>
</table>

1. ETC systems gather a great deal more information about a motorist's movements as compared to its manual counterpart. Collection of personal information should be reviewed with the aims of minimising it to a level where it reflects the true conversion from a manual to an electronic system. Embedding anonymity in the electronic process would provide better mapping, which reflects manual toll operations.

2. The current design of RFID technology in general, and ETC technology in particular, does not provide mutual authentication or encryption. The tag should be able to verify cryptographically, that the purported toll gantry reader is indeed a legitimate entity. In addition, technologies should be utilised which aim to prevent unwanted scanning of E-Tags. Privacy En-
hancing Technologies (PET) like shielding pouches or kill-switches should be implemented in transponders to prevent unsolicited scanning.

3. The strong correlation between the identity of a motorist and the unique identification of a toll tag should be minimised. An analogy here is that of a driver’s licence with the core function of confirming a motorist’s right to drive, without the need of identification. Similarly, a tag, which provides irrefutable evidence of authenticity should be sufficient proof of the use of the toll road. The tag may have a prepaid balance which may be deducted by the toll infrastructure. It would be the responsibility of the motorist to maintain sufficient credit to maintain anonymous travel. The motorist loses anonymity if the credit falls into negative balance which is analogous to fare-evasion in a manually operated toll plaza.

4. Transactions paid and settled by the motorist for a particular billing cycle should only be stored in a consolidated form per billing cycle. Historical granular transactions with identification information should either be purged or de-identified.

5. The possibility of anonymous electronic options should be actively explored. The current literature about tolls, as discussed in previous sections, seems to suggest that cash booths are at present the only option available for anonymous tolling.

6. If anonymous options exist, they should be actively advertised, alongside other options.

7. Privacy legislation should be amended to remove the exemption of privacy sector toll operators in state/territory contracts to the extent that they are not covered by privacy regulation established by the relevant state or territory Parliament, or if the relevant state or territory Parliament has weaker restrictions than the Privacy Act.
4.4 Case Study II: Mobility-Priced Insurance

PAYD is a business model for individualising insurance products. The aim is to get closer to the consumers using telematics services. Section 2.5.2 reviewed the benefits of variable insurance, ranging from reduction in accidents, fairer premiums and environmental benefits. However, the adoption of GPS technology for underwriting processes may present potential security and privacy concerns because of the collection, processing and retention of precise movement details. Are motorists being forced to save on premiums by foregoing personal privacy expectations? How long is this data stored for? Is it only used to verify the total mileage or would it end up serving other unrelated purposes? What are the privacy and security implications for the motorist if a person with malicious intent gets access to this data? Is this data stored along with identification details or stored anonymously? These are some of the questions that come to mind with regards to privacy issues in the collection and retention of GPS data. Section 4.4.1 coupled with the analysis framework in section 4.4.4 aims to address some of these questions. It also aims to make recommendations to policy makers and technology designers while GPS-enabled insurance is in its nascent stages, so that privacy protection can be built in at the design stage, rather than bolted on later.

4.4.1 Privacy Issues in Various Mobility-Priced Options

Privacy issues of the few different approaches to mobility-priced insurance discussed in section 2.5.2 are analysed in this section.

MRF and odometer audits use the total distance covered in a particular insurance billing cycle to quantify insurance premiums. This requires insurance providers to gain access to verifiable odometer readings of the insured in addition to information about driving history and experience, address, the make and model of the vehicle and where the vehicle is parked. Odometer readings of
vehicles are also used when trading cars; therefore, this has minimal privacy issues.

Incentive-based reporting systems (although voluntary) collect information about hard braking, and rapid accelerations which might be used to infer driver behaviour. The insured has the option of not disclosing this information, but recent research related to the economics of privacy suggest that people might be willing to disclose personal information for small incentives (Danezis et al., 2005; Cvrcek, Kumpost, Matyas, & Danezis, 2006). This system is more privacy-invasive than odometer auditing or MRF.

GPS-enabled insurance systems typically transmit GPS logs periodically to the insurance provider via an identifiable GSM (mobile phone) chip which can reveal a great deal more about the individual than just a calculation of kilometres driven. It can be used to record the places of interest to the driver, determine the driver’s road behaviour, perform real-time or retrospective surveillance of individuals, and create personality profiles for market-related products and services. Although GPS-enabled insurance has the highest value with regards to benefits, the associated privacy concerns defeat the technological and economical advantages it promises if its design does not reflect privacy-sensitivity.

Table 4.3: Comparison of insurance approaches for cost, privacy and accuracy.

<table>
<thead>
<tr>
<th></th>
<th>Traditional Insurance</th>
<th>Odometer Audits</th>
<th>Incentive-based reporting</th>
<th>GPS-enabled Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobility-based premiums</strong></td>
<td>Not possible</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
<tr>
<td><strong>Time of day</strong></td>
<td>Not possible</td>
<td>Not possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
<tr>
<td><strong>Risky roads</strong></td>
<td>Not possible</td>
<td>Not possible</td>
<td>Not possible</td>
<td>Possible</td>
</tr>
<tr>
<td><strong>Weather conditions</strong></td>
<td>Not possible</td>
<td>Not possible</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td><strong>Actuarial accuracy</strong></td>
<td>Inaccurate</td>
<td>Slightly better than traditional</td>
<td>Slightly better than odometer audits</td>
<td>Slightly better than incentive based</td>
</tr>
<tr>
<td><strong>Costs</strong></td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td><strong>Privacy invasion</strong></td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
With rapid developments in the field of telematics technologies, distance-based insurance would also take into account when, where and how the vehicle was driven, yielding an accurate risk model (such as incentive-based reporting or GPS-enabled insurance). These better risk models would be actuarially more accurate, but raise serious privacy issues for motorists because of the vast amounts of data collected about their road movements. Table 4.3 summarises the potential benefits and drawbacks of odometer audits, incentive-based reporting and GPS-enabled systems respectively. It seems that costs and privacy are the two issues with GPS-enabled insurance. If these can be minimised, an insurance underwriting system which is privacy-sensitive and fair can be devised.

4.4.2 Towards Legislation for PAYD

Recently, in California, US, a bill was tabled with the worthy objective of providing financial incentives to motorists who drive less. By linking automobile insurance costs directly to each decision to drive the insured vehicle, the insured would be likely to make the decision to drive less, reduce greenhouse gas emissions, and be rewarded with lower auto insurance costs (AB 2800 - Huffman, 2008).

The bill contemplated the use of GPS technology to verifiably calculate the total distance an insured drove. However, it received fierce opposition from the Consumer Federation of California in the assembly committee on insurance hearings, which argued that the bill would allow insurance companies to require drivers to install GPS-enabled devices, or pay a higher rate if they refused. This would result in mandatory GPS monitoring, since the driver would be forced to pay more for not participating in the program. The bill also did not address limiting the information collected from the GPS device, which raised significant issues regarding collection of data about driving habits and destinations not germane to the objective of verifying total mileage (Holober, 2008). This bill
was ultimately withdrawn.

Meanwhile, Californian Insurance Commissioner, Steve Poizner, who had previously pioneered a company which developed technology to put GPS receivers into mobile phones, and who understood both the benefits and threats of GPS devices, proposed legislation that would offer PAYD insurance options in California. He further added that 'I will not approve any policy that aims to utilize GPS devices to obtain location data from consumers’ (Tom, 2008). Poizner is of the view that this type of technology does not have a place in mobility-priced insurance for privacy and public policy reasons.

The proposed legislation which is expected to take effect from the end of 2009 prevents insurers from accessing location information of consumers. It does not prevent GPS-enabled insurance products that do not send any location information (only total distance) from being developed.

4.4.3 Secondary uses

Not directly related to GPS-enabled insurance, the highly publicised case of James Turner, who signed for a GPS device in his rental car with ACME, is a classic example of function creep of GPS use in the commercial automotive arena. He was fined $150 for each speeding occurrence of more than 80mph, and only became aware of this when a total of $450 was deducted from his credit card for three speeding events a month after the use of the rental car. He took ACME to court and won, on the grounds that the company had failed to clearly explain how the location tracking system would be used (Connecticut Attorney General’s Office, 2002). What is interesting to note is that the court did not condemn the technology or its use.

With the current architecture of sending GPS logs to a central server in real time, there is a possibility of a range of privacy abuses. There could be unintentional transmission of information such as how fast drivers accelerate,
how hard they brake, and how often they go above a prescribed speed limit. Similar data might even be used to establish the driver's situation just before a collision. Once the data is collected, how the information is used is limited only by the imagination of governments and multinational conglomerates, and there is not much case law to offer reassurance.

4.4.4 Analysis Framework

This section examines the privacy issues of GPS-enabled insurance, in light of the analysis framework.

**Non-Electronic Equivalence Test**

The non-electronic equivalent of GPS-enabled insurance would be a person employed by the insurance company with unlimited storage capacity, and the ability to note down vehicle location and time at extremely high granular levels (up to 10 times per second) and extremely quickly. This person would always be present in the vehicle during the billing cycle of an insurance product, and would always keep logging these movements. Every billing cycle, this person would reproduce the data and submit it to the insurer to calculate the total distance travelled. The insurer would keep a record of the total distance as well as retain all these precise movements recorded by the employee in permanent storage. With retrospective analysis, the insurer could identify the motorist from these records, and would be able to infer what was the speed of the vehicle at a particular time and date, and other driver habits.

In the case of the ACME rental car scenario, the non-electronic equivalent would be a person employed by the rental car company whose task was to follow the customer and note down the events whenever the vehicle went over the speed limit for more than two minutes.
Active vs. Passive Systems

The GPS device is switched on whenever the vehicle’s ignition is turned on. The device logs all movements in all terrains and situations. Initially the user may be aware of the presence of this device in the vehicle and might even be conscious that the device is watching their movements. But with the passage of time it would become a part of the insurer’s life, recording all movements.

Identifiability

With a GPS receiver, identity is not tightly coupled to a person because GPS is a signal reception technology, and only uses satellite signals to compute present position. However, when the GPS records of a vehicle are transmitted to the insurer, they are annotated with the policy number as well as the unique GSM chip (which would be similar to a mobile phone number) and could be used to correlate the vehicle and its movements.

Even if the GPS records were made anonymous, there would be a possibility to make inferences about the driving habits, patterns, source and destinations. As will be discussed later in Section 5.2, it is possible to identify persons from anonymous GPS data. Identifiability would not be an issue if neither GPS data nor frequent GSM communication were used for transmission.

Consent and Choice

In current GPS-enabled insurance models, a motorist provides express consent for use of the GPS data for the primary purpose of generating premiums. The motorist expects that this data will be used to calculate the total distance travelled, or in refined versions of this product, will also extract roads, times, days, and speeds for more accurate and fair premium calculations.

GPS-enabled insurance is currently not widespread; even where it is available, its use is voluntary. This means that a consumer does have a choice at this stage.
However, this may change in the future when GPS-enabled insurance becomes pervasive and the significant savings encourage consumers to forego privacy and adopt these products.

Additionally, in current models the motorist does not have the choice to prevent the logging and reporting of GPS data. Any such attempt would be considered tampering with the system and may render the insurance policy void. The motorist has no control to prevent a select number of trips to be not sent, or to be sent at a less accurate level. In short, the motorist lacks autonomy to regulate the boundaries of accessibility to personal location information.

**Locational Granularity**

GPS positional accuracy and granularity has increased over the years. With a standard off the shelf GPS-receiver it is possible to identify a position with a spatial granularity of 1-50 metres, depending on geometry and signal attenuation. As compared to the situation with tolls in Sydney, GPS location is hundreds of times more granular. Additionally, the device is capable of storing positions multiple times per second, so it can be used to reproduce the exact movements of the vehicle at a later date.

**4.4.5 Policy Recommendations**

The results from the analysis are summarised in Table 4.4. Following this there are some recommendations that are made in the light of this analysis.
Table 4.4: Summary of the analysis framework results for PAYD insurance.

<table>
<thead>
<tr>
<th>Test</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-electronic equivalence test</td>
<td>The equivalent of PAYD means an employee of the insurer is always present in the vehicle, and with indefinite storage, logs all vehicle movements in granular time intervals. All this data is reproduced for the insurer, who also maintains it indefinitely.</td>
</tr>
<tr>
<td>Active vs. Passive system test</td>
<td>GPS-enabled insurance is a passive system, which is activated as soon as the vehicle is started.</td>
</tr>
<tr>
<td>Identifiability test</td>
<td>Strong identification using the GSM chip. Even anonymous GPS data has the potential to identify people.</td>
</tr>
<tr>
<td>Consent &amp; Choice test</td>
<td>Consent provided when motorist signs up. Motorists’ sign up is voluntary, however the financial benefits may significantly influence a motorist to subscribe.</td>
</tr>
<tr>
<td>Locational granularity test</td>
<td>Extremely high precision and detail about movements available.</td>
</tr>
</tbody>
</table>

1. Given the detail of information present in GPS data about motorists’ movements, guidelines should be established that prevent the use of this location information directly by insurers.

2. Technology-driven mobility-pricing solutions should be designed which utilise the key benefits of GPS data for an accurate reflection of risk, without compromising personal privacy.

3. The GPS data stored in a motorist’s OBE constitutes personal information and access to it should be governed by established privacy laws.

4. The legal fraternity should debate the adequacy of the use of GPS data for court convictions.

5. To prevent access to GPS data stored in the vehicle’s OBE in situations such as theft, adequate security measures should be implemented that utilise encryption technology.
4.5 Summary

The aims of this chapter have been two fold: the first was to examine the key challenges faced by the two distinct yet related mobility pricing concepts and to evaluate their invasiveness by employing an analysis framework. The second was to make recommendations regarding both these applications to policy makers in an effort to restore anonymity on roads.

While there are some differences between ETC and PAYD in terms of accuracy, location granularity and the type of surveillance (active vs. passive), as summarised in Table 2.1 and 4.4, both of these systems have the capacity to embed themselves into the fabric of society and become a regular part of the citizens' lives. As mentioned in Chapter 3, these technologies can give rise to the emerging notion of Überveillance, which is an above and beyond, almost omnipresent, surveillance system (K. Michael et al., 2006). The recommendations made through the analysis framework would assuage some of these privacy concerns by holding users of this technology responsible, limiting the disclosure of precise movements and enabling autonomy and anonymity in the electronic world. It should be possible to make a meaningful contribution to society by responsible use of technology.
Chapter 5

Analysis of Threats & Vulnerabilities of GPS Data

5.1 Introduction

Chapter 4 highlighted the need for alternative design strategies for road pricing in general, and mobility pricing in particular. Before delving deeper into this task, it would be judicious to explore the vulnerabilities present in existing systems so that these problems are resolved in a future privacy-preserving model.

Taking an ‘Ethical Hacker’ approach, this chapter presents a critical analysis of threats from secondary uses of GPS data transactions, and also looks at the vulnerabilities and issues that surround the legal as well as commercial uses of GPS technology. The analysis framework presented in this chapter assumes the worst case scenario of passive data collection of the highest resolution - GPS. However, the arguments that follow are equally applicable to active, low resolution data collection systems such as toll records. Section 5.2 assesses the threats of secondary uses of anonymous GPS data to the privacy of individual motorists, followed by a critical assessment of intentional vulnerabilities that may be introduced in judicial or commercial settings, in Section 5.3.
5.2 Inferential Threats From Automated Profiling

Section 4.4.4 pointed towards the possible secondary uses of precise GPS data amassed as a result of current approaches to mobility-priced insurance systems. While theoretical research has aimed at raising awareness about these threats and proposed algorithms to protect the privacy of individuals in locational contexts (Gruteser & Grunwald, 2003; Langheinrich, 2002; Duckham & Kulik, 2005), all these countermeasures are rendered ineffective in the case of GPS-enabled insurance, where premiums are currently priced on the basis of full disclosure of precise GPS data. This section aims to demonstrate the threats of inferring behaviour and personalities from ‘anonymous’ GPS data by means of a data collection exercise. A software is implemented that takes this GPS data as input, and generates a range of personal information about an individual including their home address, social life, work activities and driving behaviour, using various heuristics. The primary motivation here is to establish a threat model for anonymised GPS data used in conjunction with heuristics and existing geographical databases, and to analyse the magnitude of these risks to personal privacy from automated data-mining.

Ashbrook et 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 locations of importance from the GPS data and used it to design an intelligent predictive model of the user’s future movements.

Krumm (2007) developed a similar protocol, and tested it to identify the home location and to infer identities of 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 also applied the theoretical countermeasures
already present in location privacy research on these locations to verify their
effectiveness.

K. 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 the use of GPS with civilians, and points
out that adequate safeguards need to be in place to avoid the abuse of information
gathered through GPS technology.

Greaves et Gruyter (2002) discuss how a driving profile of a person can
be derived from GPS track data. They sought an understanding of driving
behaviour 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.

5.2.1 Inference Attack

An Inference Attack is a data-mining technique where analysis of lower level visi-
table data enables the deducing of higher level sensitive information (Morgenstern,
1987). Inference problems differ from other security problems in that it is not
an issue of unauthorized access to data, or of leakage of information. Rather, a
subject’s sensitive information can be considered as leaked if an adversary with
access to trivial information at a lower security level can determine a fact that
should be protected at a higher security level.

In the GPS data context, the purpose here is to explore the possibility of
deducing identity and behaviour from anonymous data. Thus the storage and
retention of even anonymous data may become a potential threat if subject to
inference attacks.
5. Analysis of Threats & Vulnerabilities of GPS Data

5.2.2 Threat Model

The threat model chosen here is of a passive, attacker-centric nature, given that GPS data collection is a passive data collection system. The attack model simulates a typical adversary's three main moves as shown in Figure 5.1. The first step is information collection using passive surveillance. This step is followed by an inference attack by performing analysis of intercepted data by using data-mining, pattern recognition, and reverse geo-coding of significant locations. Finally in the third step, the adversary performs profile generation and infers behaviour and identity of individuals.

5.2.3 Apparatus

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 the choice of a passive GPS device known as the TrackStick Pro™ as shown in Figure 5.2(a). This GPS stick uses power from the cigarette lighter in the car and has a memory of 4 MB, which is suitable for storing the track data for up to a period of one month. Once the device is connected to the cigarette lighter, it turns on when the vehicle's ignition is switched on and starts logging data without any user intervention or input.

The GPS device came with a software utility, which enabled it to be configured for use in a vehicle and offered a capability of logging location, time, date, speed, elevation and temperature data at a rate of 6 times per minute. Although
5. Analysis of Threats & Vulnerabilities of GPS Data

(a) The GPS tracking device used in the experiment.

(b) The GPS device installed and operational.

Figure 5.2: Details of the GPS device used.

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.

5.2.4 Passive Surveillance

The five volunteers selected for this study were an undergraduate student, a research student, an academic staff member, and two support staff from the school. 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 5.2(b), volunteers were taught how to fix the GPS stick to their vehicle’s dashboard using double-sided tape and to connect the power plug to the cigarette lighter jack. The GPS device had to be placed in such a way that it had line-of-sight to the GPS satellites. The volunteers were advised not to remove the stick or the power source for the period of study. At least one week’s 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 (Wigan & Clarke, 2006).
5. Analysis of Threats & Vulnerabilities of GPS Data

<table>
<thead>
<tr>
<th>Rec #</th>
<th>Date</th>
<th>Time</th>
<th>Latitude</th>
<th>Longitude</th>
<th>Altitude</th>
<th>Status</th>
<th>Course</th>
<th>GPS Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>134</td>
<td>03/17/2007</td>
<td>11:15</td>
<td>-33.9123°</td>
<td>151.1194°</td>
<td>24.7 m</td>
<td>NE</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>03/17/2007</td>
<td>11:22</td>
<td>-33.9054°</td>
<td>151.1275°</td>
<td>0.0 m</td>
<td>Power On</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.3: GPS track data downloaded onto PC from GPS device.

5.2.5 Interception and Analysis

Data Cleansing

On completion of the specified period, the GPS data was downloaded to the PC and stored anonymously without identifying the volunteer in any way. Any errors in data collection were rectified; for instance, unusual speed or location values.

Significant Locations Analysis

The second step in the analysis was to identify significant locations from the data. A simplified approach was adopted for collating significant locations. As shown in Figure 5.3, 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) represents 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.

This algorithm was implemented in Visual Basic.net. The purpose of choosing this programming language is that there is a set of Application Programming Interface (API) available in this language that programmatically allows connec-
Algorithm 1 Extract Significant Locations

**Input:** GPS Log File from a volunteer

**Output:** Significant Locations

1. while GPS Log File is not empty do
2. GPSRow = Read A GPS Row
3. if GPS Status (GPSRow) = 'Power Off' then
4. GPSPreviousRow = Read Previous GPS row
5. GSTime = GetTime (GPSPreviousRow)
6. LocationXY = GetLocationXY(GPSPreviousRow)
7. if GSTime Between 3pm to 10 pm then
8. Significant Locations = Significant Locations + LocationXY
9. end if
10. end if
11. end while
12. return Significant Locations

...tion to the GIS software for further analysis and profiling. As summarised in Algorithm 1, all the locations prior to the ‘Power Off’ signal were selected in an effort to identify the home locations. Since all the volunteers were associated with the university, the algorithm does not compute the work locations and focused on 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 trips would end at the home locations during this time period.

Inferring Home Location via Reverse Geo-coding

To find the nearest street address to the significant locations, the PSMA Geocoded National Address File (GNAF) index was used. This address file contains the geocode (specific latitude and longitude) of all physical addresses in Aus-
Figure 5.4: GNAF data model. Source: (GNAF Product Description, 2009)
Algorithm 2 Reverse Geocoder

Input: List of significant locations (X,Y) pair

Output: List of street addresses

1: for all i in the list of significant locations do
2: Query GNAF database and get the nearest street address to i(x,y)
3: StreetAddress = address, suburb, postcode, and street number
4: StreetAddressList = StreetAddressList + StreetAddress
5: end for
6: return StreetAddressList

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 magnitude of storage requirements, GNAF data for only NSW was loaded into the database, exceeding 5 Gigabyte (GB) of storage space alone. The data import utility which comes with GNAF was used to import tables and data into PostgreSQL.

Figure 5.4 shows the data model of GNAF. Using this model a reverse-geocode utility was developed that returns the closest street address to a particular coordinate pair (x,y) within a given radius. It was assumed that the vehicle would be within 10 metres of the person’s street address. Using Spatial SQL the filtered significant positions obtained from the previous section were requested from the database, and returned street addresses nearest to those points. This process is illustrated in Algorithm 2. The statistical mode (most frequent) was used to short-list the physical addresses of the volunteers. Since the mode is not necessarily unique, the physical address computed by the protocol could be more than one.
Table 5.1: Protocol output of inferred home location compared with actual street address obtained from post-exercise interview.

<table>
<thead>
<tr>
<th>Home Location</th>
<th>Volunteer C</th>
<th>Volunteer B</th>
<th>Volunteer Y</th>
<th>Volunteer J</th>
<th>Volunteer U</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inferred Street Number</td>
<td>7</td>
<td>39</td>
<td>24,25</td>
<td>44</td>
<td>53</td>
</tr>
<tr>
<td>Actual Street Number</td>
<td>11</td>
<td>39</td>
<td>22</td>
<td>Different street</td>
<td>51</td>
</tr>
</tbody>
</table>

5.2.6 Profile Generation

Home location results

The automated inference attack presented in Section 5.2.5 yielded a set of street addresses for each volunteer. Only first initials of the volunteers were 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 to where they actually lived, which according to the assumption falls within the 4 address buffer range. The volunteers were shown the final results and were asked to verify whether the home determination algorithm’s results coincided with their actual street address. Table 5.1 summarises these results.

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 was recorded on the road closest to the street address as shown in Figure 5.5.
Inferring Additional Details

Since the volunteers were known, it was also possible to use the compiled list of street addresses and the list of names to gain further information. Although not shown in this exercise, it was possible to access web-based ‘White Pages’, and get access to additional details of volunteers. As shown in 5.6, an intersection of the volunteers’ names and street addresses can yield residence telephone numbers (if listed) quite easily.

Heuristics-based Reporting

After inferring the street address of the drivers, the next stage was to use the same data and make inferences about their social and work related activities. The whole GPS track data was sifted and aggregated by the software program, and the output of this step is summarised in Table 5.2. 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 at their home. This infor-
information can be used by adversaries with malicious intent. Krummi (2007) has extended this concept 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, which may be used to measure travel-related stress or risk.

Volunteer ‘Y’ seemed to spend the longest time at the university and lived the farthest distance away. On average he/she had to travel approximately 40 kms. to commute to work and back home each day. The algorithm was 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 parks at the university parking lot is privileged with a parking permit (and is either an academic, support or research staff/student).

Another heuristic used was that if a person parks within a 2 km buffer around the university, then he/she does not have a parking permit and is most likely an undergraduate student.
Table 5.2: Profile Summary of volunteers generated by the software protocol.

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Volunteer C</th>
<th>Volunteer B</th>
<th>Volunteer Y</th>
<th>Volunteer J</th>
<th>Volunteer U</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total GPS records</td>
<td>5240</td>
<td>1997</td>
<td>2330</td>
<td>4812</td>
<td>2147</td>
</tr>
<tr>
<td>Total distance</td>
<td>301 km</td>
<td>174.59 km</td>
<td>172 km</td>
<td>284.9 km</td>
<td>149.7 km</td>
</tr>
<tr>
<td>Avg. distance</td>
<td>27.4 km</td>
<td>34.6 km</td>
<td>31.2 km</td>
<td>40.7 km</td>
<td>37.4 km</td>
</tr>
<tr>
<td>Total travel time</td>
<td>12h 45m</td>
<td>4h 25m</td>
<td>5h</td>
<td>11h 44m</td>
<td>4h 51m</td>
</tr>
<tr>
<td>Avg. daily travel</td>
<td>1h 10m</td>
<td>52m</td>
<td>54m</td>
<td>1h 40m</td>
<td>1h 12m</td>
</tr>
<tr>
<td>Max speed</td>
<td>101 k/h</td>
<td>83 k/h</td>
<td>86 k/h</td>
<td>98 k/h</td>
<td>91 k/h</td>
</tr>
<tr>
<td>Avg. speed</td>
<td>32 km/h</td>
<td>45 km/h</td>
<td>39 km/h</td>
<td>33 km/h</td>
<td>39 km/h</td>
</tr>
<tr>
<td>Avg. time</td>
<td>07:33</td>
<td>08:21</td>
<td>09:10</td>
<td>07:46</td>
<td>09:54</td>
</tr>
<tr>
<td>leaves home</td>
<td>15:30</td>
<td>17:09</td>
<td>16:54</td>
<td>20:58</td>
<td>17:07</td>
</tr>
<tr>
<td>leaves work</td>
<td>7h 58m</td>
<td>8h 10m</td>
<td>7h 25m</td>
<td>12h 18m</td>
<td>6h</td>
</tr>
<tr>
<td>Parks Car in</td>
<td>University</td>
<td>University</td>
<td>University</td>
<td>University</td>
<td>Around</td>
</tr>
<tr>
<td></td>
<td>parking lot</td>
<td>parking lot</td>
<td>parking lot</td>
<td>parking lot</td>
<td>campus</td>
</tr>
<tr>
<td>Type of person inferred</td>
<td>Academic</td>
<td>Academic</td>
<td>Academic</td>
<td>Research</td>
<td>Undergrad</td>
</tr>
<tr>
<td></td>
<td>or Support</td>
<td>or Support</td>
<td>or Support</td>
<td>student</td>
<td>student</td>
</tr>
</tbody>
</table>

Driver Behaviour Analysis

In this section speed and acceleration analysis was 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.

Intuition suggests that individual driving behaviour is a function of many factors, such as the 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, McLean, Moore, & Ponte, 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 ESRI’s 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.

At this stage the GPS data was programmatically converted to ESRI Shapefile format, which is the preferred file format for ArcGIS, Version 9.2. All the records from the GPS data that had the 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 give positional information of the preceding GPS record. These would prove useful in demonstrating the idea of significant locations spatially, as 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.

Figure 5.7 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 $\pm3m/s^2$ at a certain stage, which is considered risky according to prior research (Greaves & Gruyter, 2002; Watson, 1995). 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 $\pm 3m/s^2$ are considered to be a source of increased fuel consumption and emissions and may be used to identify the driving behaviour of individuals.

Figure 5.8 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 in the home inference algorithm. Note the black dots around the university vicinity, where the volunteer had parked the car frequently which were used to predict if the volunteer was an undergraduate student. The red dots indicate that the speed exceeded 80 kph on those road sections. With access to speed data of all the roads, it could be easily inferred if an individual was over the speed limit. It is also not hard to imagine that if insurance companies

Figure 5.8: GPS track data downloaded onto PC from GPS device.
get access to this data, they could possible use this information, to identify an individual with an 'aggressive' driving style and assign the individual a higher risk ranking, leading to a higher premium.

5.2.7 Evaluation

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. All of this was achieved using completely anonymous data and following the most simple approaches, yet the protocol was still able deduce patterns, infer address details of the volunteers, and draw up summary profiles. This exercise is evidence of how much personal privacy could be eroded when professional data-mining services of GPS data are employed using various techniques and approaches. The promise of storing data anonymously is not sufficient to counter these concerns.

Personal Information

Personal information, according to the Federal Privacy Legislation means

"information or an opinion ... about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." (Privacy Act 1988, 2008)

The profiling exercise looked at various aspects of the volunteers' lives and predicted what class of personnel they belonged 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. This means that in these circumstances, anonymous data can lead to the decertification of individuals and constitutes personal information.
Sensitive Information

Definition of sensitive information as per the Privacy Act was reviewed in Section 3.4.2. There are higher standards in the collection and handling of sensitive information. Often it also requires the explicit consent of the data subject.

Inferences made using location data can be used to harm an individual and may prove embarrassing to him/her when revealed publicly. For instance, using the significant location approach discussed in this chapter, the ‘points of interest’ of an individual may be reverse-geocoded and the address looked up on web-based maps to infer what those locations are. If those points of interest include locations which reveal a person’s religious affinity, sexual orientation or membership to a professional organisation, this becomes sensitive data. Even though the GPS data was anonymised in this setup, it has been established that it can be used to infer identities as well as sensitive information.

5.2.8 Recommendation

Rigorous ethical and legislative safeguards need to be implemented to protect future abuses of individuals’ privacy in locational contexts. 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 made integral to them. With regards to payment models that depend on GPS disclosure, different techniques should be explored that balance community privacy expectations and accuracy requirements for payment processing.

As established in previous sections, location-based applications which require complete disclosure of GPS data would be highly vulnerable to abuse even if the data is de-identified and then stored, because of the complex nature of the ‘spatio-temporal footprint’. The access and availability of disparate geo-
informational databases make it easy to gain both personal and sensitive information about individuals. Therefore in the context of GPS-based transaction processing it is extremely important to explore alternative designs that do not disclose precise GPS information to a third-party.
5.3 Legal & Ethical Implications of GPS Vulnerabilities

In recent years, the legal system has encountered various cases involving the use of GPS data presented as evidence. In the US, courts have debated whether surreptitious installation of GPS-tracking devices amounts to invasion of privacy of individuals. However, there has been minimal discussion about the accuracy of this GPS data in legal contexts, and virtually no mention in judicial reasoning of the vulnerabilities of GPS data as a result of malicious human intervention.

GPS is a radio-navigation system and is prone to certain vulnerabilities that may be introduced intentionally or unintentionally (Volpe, 2001). This section describes experiments conducted to highlight two weaknesses of GPS systems which may be introduced intentionally: specifically, malicious editing of GPS data, and spoofing of GPS signals, which means the transmission of GPS-like fake signals with false positional data. These issues raise the prospect of forged GPS data being presented to courts by individuals who have the motives and the technical knowledge to inflict harm, to defame or to exonerate a person of criminal charges. By exposing the weaknesses present, the aim is to draw the attention of the legal fraternity to these issues which may present the legal system with dilemma, since over-reliance on GPS technology in judicial settings may produce disastrous results, especially when innocence or guilt largely depends on GPS evidence.

5.3.1 Legal Scenarios

Tracking by Law Enforcement Agencies (LEA)

The US Constitution’s 4th Amendment protects the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures (Kilman & George, 2000). The fourth amendment test has been applied
in various cases to decide whether the privacy rights of individuals were violated. The Supreme Court case that comes closest to the use of GPS tracking is that of the United States vs. Knotts (1983), involving a beeper - a battery operated RF transmitter, which was attached to a chloroform container that the defendant had purchased and loaded in his car. The police followed the defendant by a combination of visual surveillance and the use of the beeper to locate the defendant’s rural cabin, which turned out to be a drug laboratory. Although a search warrant had been obtained to enter the premises, the court held that monitoring the vehicle while it was on public roads without a warrant was permissible because the defendant had no reasonable expectation of privacy when in public. According to the court, the beeper was merely ‘an augmentation to the sensory faculties bestowed upon the police officials at birth’, (United States vs. Knotts, 1983) and was analogous to using a pair of binoculars while conducting visual surveillance.

The United States vs. Garcia (2007) case is a more recent one and directly involves the use of GPS data for the surveillance of suspected criminal activity and largely draws on the Knotts case. The police were tipped off by an informant that the defendant, who was recently released from prison for methamphetamine (meth) offences, had mentioned to him that he intended to produce meth again. The police located the defendant’s vehicle on a public street where it was parked, and fitted a GPS memory tracking unit under the rear bumper. After a few days, when the device was removed, the police were able to learn the car’s travel history since installation, which led them to a tract of land that the defendant frequented and which contained equipment and ingredients to produce meth. The defendant was arrested and charged with drug offences. The defendant demanded the suppression of this evidence as being the fruit of an unconstitutional search, since a warrant had not been obtained before installing this tracking device. The 7th Circuit Court of Appeals concluded that installation of the GPS tracking device
neither constituted seizure nor search, because the device did not interfere with the driving qualities of the vehicle and was analogous to a police officer following the vehicle. However, the court did acknowledge that there was a practical difference between following a vehicle and using GPS devices.

Tracking by a suspicious spouse

Another extraordinary case that has recently come to light involved the use of a GPS tracking device by a suspicious wife in her husband’s vehicle (Finz & Taylor, 2004). The data obtained from the tracking device led to the filing of murder charges by the police in the death of the couple’s twelve year old baby-sitter. The device had been placed by the wife in her husband’s truck a few days earlier because she suspected him of having an affair. The husband told the police that he went to drop the baby-sitter to her home when they took a detour to show her some horses, then accidentally ran her over as he turned his truck around on a rural road in Central New York. He was initially charged with a felony count of reckless endangerment, but based on data obtained from the GPS unit the charges were raised to second degree murder as data revealed that the defendant had not taken the girl to see horses at all. Instead, he drove around other roads and spent more than three hours with her behind an abandoned home. Police believed that the girl had got away from him when he drove over her. At the time of writing this thesis, this case awaits a decision, but it is clear that GPS data was the major evidence used for indictment.

Parolee Tracking

GPS has become the technology of choice for implementing parolee and sex-offender tracking. At least twenty-three states in the US use GPS tracking of convicted sex-offenders, and some states are even using GPS tracking as an inexpensive transition program for low-risk offenders, in order to make more room
in the crowded prisons (Mohan, 2006). Usually worn as an anklet or bracelet by the parolee, GPS tracking has proven to be a powerful tool in strengthening the monitoring of high-risk offenders (Newschannel.com, 2007).

From real-time and retrospective monitoring of a subject’s locations, movement patterns can be developed, and unusual activity may be predicted, as seen in 5.2. Additionally, by augmenting the tracking device with additional sensors, future models of these bracelets will also be capable of sensing the presence of drugs and alcohol and of transmitting this information to a monitoring facility in near real-time (Questguard, 2007). These controlled efforts to weave ex-offenders into the fabric of society requires monitoring and can be valuable, but it is open to debate whether it violates the privacy rights and would motivate them to tamper with these devices.

**GPS Admissibility as Evidence in Liability Offences**

In the context of liability offences, there have been instances where motorists have successfully challenged the issuance of speeding tickets against them by providing GPS data as evidence (Wainright, 2007). Recently, a motorist in NSW was fined $203 for allegedly driving at 85 km/h in a 60 km/h zone. The motorist challenged the fine in court and presented data from his on-board GPS navigator which showed that he was mostly travelling at a speed of 57 km/h on that particular stretch of the road, which was also corroborated by a GPS expert in court. The motorist challenged the accuracy of the hand-held radar guns, questioning how rigorously these guns were calibrated each year. The traffic officials conceded in court that they had not taken the readings on their radar guns for the required length of time and had simultaneously relied on their experience and visual estimates. The fines were overturned in the district court setting a precedent for the admissibility of GPS evidence in NSW.
5.3.2 Commercial Scenarios

It was discussed in Chapter 2 how transactions, such as mobility-pricing, electronic parking, electronic tolls and congestion charging, have started depending on positional data. In the United Kingdom (UK), the London congestion charge has been operational for some time and uses ANPR. There are suggestions to give additional discounts to motorists who opt for GPS-based charging. There are speculations that the British government has engaged with an insurance company offering mobility-priced insurance in an effort to acquire GPS data of its clients for its own GPS-based congestion-charging research (Hytch, 2007).

While it has been discussed that GPS-based charging would be fairer and help ease environmental problems such as congestion and pollution, it is also possible that a technology-savvy person may seek the means of cheating the system to gain additional savings, or to rebel against such a charge. In the UK, for instance, ‘car-cloning’ is a technique being used by cheaters to avoid congestion-charges and camera-based enforcement systems. Law-abiding citizens are inadvertently being fined and often experience difficulties in getting the police to take the matter seriously and/or having the fines overturned (BBC Inside Out, 2005).

5.3.3 Vulnerability Assessment

The situations discussed in Sections 5.3.1 and 5.3.2 may motivate a person to tamper with or erroneously edit the GPS data contents in order to evade criminal charges, avoid financial liability, cheat mobility-pricing systems, provide false GPS alibis, escape speeding fines, frame another person for committing a crime, or simply misinform employers of their whereabouts. These motivations are significant enough to warrant a critical assessment of GPS vulnerabilities to intentional interference.

The Volpe (2001) report discusses these vulnerabilities, ranging from ionospheric interference and RF interference, including television broadcasts and
Very High Frequency (VHF) interferences causing unintentional disruptions, to jamming, spoofing and meaconing of GPS data in intentional disruptions, as summarised in Figure 5.9. The Ionosphere surrounding the earth approximately 350 kms away refracts GPS signals transmitted from satellites and may introduce certain errors in the position solution. Likewise, RF interference from TV and VHF transmitters may interfere with GPS receivers at ground level.

Jamming, spoofing and meaconing, as mentioned earlier, form intentional disruptions to GPS operations. *Jamming*, as the name suggests, means emission of radio signals of sufficient power to prevent receivers in the target area from tracking GPS signals. *Mecaconing* is the reception, delay and rebroadcasting of radio-navigation signals to deceive the GPS receiver. *Spoofing* is a technique to deceive the receiver into locking onto legitimate-appearing false signals and making it believe that it is somewhere else.

No evidence has been found of any prescribed standard or practice of assessing vulnerabilities, either in law enforcement environments or the commercial sector for the suitability of a GPS device for a specific task. This study questions the over-reliance on GPS data in legal proceedings and the commercial sector
by arguing that these susceptibilities can be exploited to significantly or totally change the positional claims in the stored GPS data.

5.3.4 Threat Model

Using off-the-shelf, commercially available GPS devices, two classes of intentional attacks to GPS receivers are demonstrated. The first scenario consists of 'malicious editing attacks', where the GPS receiver is not packaged in a tamper-proof enclosure and its removal would not raise any suspicions. The second scenario exploits the spoofing attack, where physical access to the GPS receiver is made difficult because of tamper-proof packaging. Figure 5.10 shows the threat model where editable logs and insecure storage exposes the former malicious editing scenario, and spoofing exposes the latter.

5.3.5 Apparatus

Four different commercially available GPS tracking devices were used to conduct the experiments, as shown in Figure 5.11. Two of them had serial flash memories. (Figure 5.11: yellow and red borders) to log the GPS data on the same
board as the GPS receiver. One of the devices had a Personal Computer Memory Card International Association (PCMCIA) interface to a Personal Digital Assistant (PDA) and stored National Marine Electronics Association (NMEA) format messages on the file system of the device (see Figure 5.11: green border). The last one was a Bluetooth GPS receiver that transmitted NMEA messages to any paired Bluetooth device, e.g. a Bluetooth-enabled mobile phone, laptop or PDA (see Figure 5.11: blue border). With the exception of one of the tracking devices, which utilised power from the cigarette lighter adapter of the vehicle, all devices had self-contained power sources (see Figure 5.11: blue border). All the receivers had 12 parallel satellite tracking channels, with accuracies ranging between 15m and 22m on the horizontal plane and a price tag of under $US 250.

5.3.6 Malicious Editing

GPS receivers process the signals they receive from satellite transmissions and compute positioning solutions. The results are stored in storage memory. The way current storage memories are designed exposes them to certain vulnerabilities. GPS devices lack any cryptographic protection for the tracks, routes and
waypoints stored in its memory, and a compatible software tool can be used to edit the positional data. There is no method to validate, for the purpose of non-repudiation, that the claimed GPS positions on file were indeed generated as a result of the GPS receiver processing.

This experiment involved editing the GPS data, and a volunteer was required to install the GPS devices in a vehicle to collect data. An administrative staff member from the School, with little technical knowledge about these devices, was asked to take them with him in the School's car when he left on a trip to conduct some work-related tasks. These devices were powered-on and were attached to the front dashboard of the vehicle using double-sided adhesive tape. The antennas of the GPS receivers had line-of-sight to the open sky. The volunteer brought back all the four devices after completion of the trip, and reported that he had visited the bank and an office goods supplier before returning to the University.

**NMEA messages output to the file system**

Two of the GPS receivers generated NMEA output, which was connected to a mobile phone and PDA respectively. The NMEA output was stored as text files on the file system of the mobile phone and the PDA. The NMEA format was primarily developed as an interface between marine electronic equipment and therefore its contents are not intelligible to people. However, there are software converters available that can convert from NMEA format to various other data formats (for instance GPS eXchange Format (GPX), Keyhole Markup Language (KML), Shapefile, Comma-separated values (CSV)), which makes this data comprehensible to users. Using editors for these formats, the data variables including positions, speed and the times can be altered and then translated back to NMEA, and the same file can be overwritten with the edited contents. There is no method to verify that the contents of the NMEA file are produced as a
result of the GPS receiver’s processing.

This technique was used to edit the contents of the NMEA files created as a result of the volunteer’s trip. On the return leg of the vehicle, a fake stop-over was added, right in-front of a sports-bar (see Figure 5.12). The data was edited so as to report that the vehicle was parked in this compound for 30 minutes before proceeding back to the University. When the volunteer was shown the fake stopover on a spatial map, he rightly denied it, but did not have any answer as to how it may have occurred. It was then explained to the volunteer that the deception involved in this experiment was not to vilify him, but rather to expose the vulnerability.

Binary data stored on flash memory

In this scenario the tracking devices stored the GPS data in proprietary binary format on flash memory. Figure 5.13 shows the receivers without casings. The
flash memory is circled yellow and the USB interface is circled red in the picture. The USB interface allows connecting the GPS device to be connected to a PC for data extraction. Both these devices come with software that caters to data export into different formats on the PC. The user interfaces provide only read-only access to the flash memory on these tracking devices. Editing the GPS logs in this case seemed difficult as compared to the previous scenario.

Further investigation of these flash memory chipsets led to the realisation that they are general purpose serial flash memory chips and can be used in a range of devices, including mobile-phones. The data-sheet specifications for them are widely available, explaining how to write binary data onto them (Atmel, 2007). These flash memories are not secure, and do not have any measures to indicate if they have been tampered with. If a technically savvy person with basic electronics skills is able to decipher the format that the manufacturer used to store GPS data, it is possible to reprogram the contents of the flash memory using the same USB interface that is used to download the data to a computer. Alternatively, as the tracking devices are commercially available, it is not difficult
to obtain an additional GPS receiver of the same specification and to use it in a vehicle to create a desired route so that the flash memory has the required data. Then either a swap of the boards or a swap of the flash memory makes it possible to put different contents on the tracking device.

5.3.7 Spoofing Attack

A spoofing attack, as explained in Section 5.3.3, is a sophisticated attack on an individual GPS receiver where a transmitter is used that sends signals very similar or identical to what GPS satellites would be transmitting. If transmitted at a slightly higher power level than the actual satellite signals, it is possible that the GPS receiver locks onto these signals and eliminates the actual satellite signals as interference or noise while computing position solutions. Figure 5.14 illustrates the threat scenario, highlighting the key input stage where fake GPS signals could be added. Volpe (2001) reports that spoofing attacks would most likely be targeted towards individuals instead of large areas.

For GPS receiver research and design, various research facilities have access to GPS signal generators. These simulators generate RF signals for different
conditions in order to test the performance of receiver algorithms in situations involving interference, e.g. multi-path. These signal simulators can be used to conduct a spoof attack on receivers, as they are capable of emulating the same Pseudo Range Number (PRN) of the existing satellites.

A Spirent 6560 multi-channel GPS signal generator was used to generate a high-gain RF signal (see Figure 5.15). This RF signal was outputted to a re-radiator antenna on the ceiling of one of the lab rooms (see Figure 5.16). In order to mimic actual vehicular movement, logged NMEA data obtained by driving a car equipped with a GPS receiver was brought back to the lab, and was used to create a scenario in the signal simulator. This means that the output obtained from the re-radiator antenna can make a GPS receiver believe that it is in motion, and the GPS receiver’s processed data can be used to verify that it acquired the spoofed signals, showing that the GPS receiver followed the vehicle’s track.

With the exception of the tracking device that required power from the cigarette lighter, all 3 GPS receivers were placed beneath the re-radiator antenna. The scenario was then run on the GPS simulator, which sent the RF signal output of the satellite signals in such a way that it represented a vehicle’s motion on the roads when processed on the receiver. All the three receivers processed the signals emitted from the signal generator and computed false positions, thus validating Volpe’s inference about commercial receivers’ inability to detect spoof attacks (Volpe, 2001, p. 39).
5.3.8 Evaluation

The conducted exercise verifies the hypothesis that it is possible to tweak GPS data either by physically tampering with it, or by the use of more complicated spoofed signal attacks. Although it requires adequate technical knowledge to perform these hacks, the possibility cannot be ruled out. This research demonstrates that GPS data can be edited to portray a different scenario, which may be used to substantiate that a person was not going over the speed limit, or was at a friend’s place at the time of a crime incident, or an employee for a courier company was busy with delivery of orders, whereas in reality a different event may have occurred. The cases and circumstances discussed in Sections 5.3.1 and 5.3.2 may act as a perfect motive, tempting a person to tamper with the GPS devices in order to prove innocence or guilt.

Consider the United States vs. Garcia (2007) case in the light of these exposed vulnerabilities. Garcia was under GPS surveillance on suspicion that he had an intention to produce meth again. The tracking device was installed under the plastic bumper of his vehicle when it was parked on a public street. Had he known about the presence of the tracking device, he might not have travelled to the drugs laboratory site to raise further suspicion and avoid arrest. It is possible
to imagine that he would have shielded the GPS antenna of the tracking device to prevent its operation. It can also be speculated that he would have sought technical assistance in cheating the GPS device, by either physically editing the data on the tracking device or by conducting a spoof attack which would have resulted in the GPS device logging the motion of the vehicle on roads of his choice, resulting in the reversal of these suspicions and eventually misleading the police about his plans. Even if sophisticated tracking devices which transmit locational information in near real-time using the GSM network were used, a carefully planned spoof attack reporting locations within the same mobile cell would have circumvented precision tracking, yielding fewer details.

The same analogy can be applied to the other scenarios discussed. For instance in financial liability matters, such as the temptation to evade a speeding fine, a person could be motivated to edit GPS data contents to prove that no offence occurred. Individuals may also not appreciate the idea of mobility-pricing of roads (for insurance or a congestion charge) where a fee is applicable based on the distance covered, and may rebel against it by trying to outwit the system by exploiting these weaknesses.

5.3.9 Countermeasures

In order to strengthen GPS systems against these weaknesses, several countermeasures can be implemented, both in terms of policy as well as technology development. With regards to policy, it is clear that GPS output which is not exclusively read-only, whether in the form of NMEA messages or any other standard or proprietary format, should not be admissible in court as evidence, due to its high susceptibility to tampering. Tracking devices that store GPS logs in proprietary binary format on the same board as the GPS receiver, and provide read-only access, can still be edited with the correct know-how and tools, and therefore expert advice should be sought when assessing these types of devices.
5. Analysis of Threats & Vulnerabilities of GPS Data

in court proceedings.

One possible solution to this problem may be to introduce cryptographic techniques to the storage process, where GPS logs are encrypted and digitally signed (Goldwasser, Micali, & Rivest, 1988) so that it can be verified that the data has been produced exclusively as a result of the GPS receiver processing and that no other GPS receiver could produce those same results.

However, building in encryption and non-repudiation into the GPS hardware cannot prevent spoofing attacks. Several countermeasures against spoofing have been proposed in the literature (Volpe, 2001; Lagier, Craig, & Benshoof, 2004). These include GPS receivers constantly measuring the Received signal strength (RSS) of the satellite signals, and if significant difference beyond a certain threshold is found between the expected and observed signal strengths, the user can be alerted to a possible spoof attack. This countermeasure fails if a sophisticated attacker also monitors the RSS and transmits its signals within the threshold, but at a slightly higher strength than the observed RSS. This countermeasure also fails if the person who owns the GPS device is the one tampering with it. Other similar solutions include angle of arrival discrimination, amplitude discrimination, time of arrival discrimination, and cryptographic authentication (Volpe, 2001, p. 39).

Military-grade GPS receivers use encrypted signals known as Precision Code (P-Code). These signals work on top of the Course/Acquisition (C/A) code available for civilian users, and can be unscrambled only by US military GPS receivers, providing greater accuracy and robustness. In view of the increased reliance of civilian transport infrastructure on GPS, there are suggestions to introduce signal authentication for civilian use in order to mitigate spoofing attacks (Hein, Kneissl, Rodríguez, & Wallner, 2007). However, it is unlikely that these hardware, software and infrastructure extensions will be available to civilian GPS receivers in the imminent future.
For applications such as mobility-based charging, where transactions depend on accurate processing of GPS data, tamper-proof hardware needs to be installed that prevents the owner or user of a vehicle from hacking into the system. The GPS device can be augmented with other sensors, such as an accelerometer, and the odometer output can be compared to the GPS velocity to verify if the vehicle is actually in motion.

5.3.10 Recommendation

An important issue that has not been thoroughly examined before, has been addressed here, namely, the vulnerabilities of GPS systems and their implications in judicial reasoning and commercial settings. While GPS data have been used as an effective tool in generating suspects, deterring criminal activities, repressing behaviour, and improving response times, the exposed vulnerabilities bring into question all such scenarios. By highlighting that the seriousness of such issues can be a motive for adversaries to exploit these susceptibilities to their favour.

The common perception that GPS is 'generally valid' means that there is an implicit over-reliance on this technology, while the conducted experiments have demonstrated that such over-dependence may prove disastrous. In the context of GPS-based pricing these threats become even more real when people may seek methods to cheat this system and avoid payments. It is recommended that GPS-based pricing approaches take these vulnerabilities into account and that systems are designed that are tamper-proof as well as being capable of withstanding intentional attacks. This is also in accord with Section 5.2.8 where alternative privacy-protecting strategies that aim at minimal disclosure have been recommended.
5.4 Summary

Two different but related issues have been explored in this chapter. One is the exposure of threats of automated inferencing from GPS data in secondary-use contexts. This is a critical issue and highlights the fact that GPS-enabled transactions, such as mobility-priced insurance collecting of high resolution movement data for accurate charging, could create a precise movement database that would act as a massive ‘honeypot’ for function creep. This means that payment models that use GPS for accurate reflection of usage need to employ a federated approach rather than a centralised one since it has been demonstrated here that even anonymising GPS data in a centralised setting does not solve the problem.

The second issue focuses on the possibility of cheating a GPS-pricing system in order to evade payments. This issue is equally applicable to both centralised and federated approaches, but is even more important for models where no disclosure of GPS data to a provider takes place, as the provider implicitly trusts the federated system to collect accurate charges on its behalf. For mobility-priced insurance, if it can be guaranteed to the insurance provider that a system exists that accurately charges the correct insurance premium on vehicles instead of transmitting it back to the server, most of the privacy issues discussed could be assuaged.

The best privacy protection is to not keep personal information in the first place, and that is the point made in this chapter. Both issues discussed here are critical, and warrant that a privacy-aware mobility-pricing system should minimise disclosure of granular position information as well as being packaged in a tamper-proof enclosure guaranteeing accurate pricing.
Chapter 6

Methodological Assessment of User Perspective of Telematics

6.1 Introduction

In 2006 the ALRC published an issues paper on privacy matters (Australian Law Reform Commission, 2006). That document mentioned that organisations that implement systems which do not enable anonymous transacting with individuals generally will not be required to comply with NPP 8 because it would not be ‘practicable’ to alter such systems to cater for anonymity. This issues paper also sought submissions on whether the anonymity principle should have a stricter implementation in the process of privacy law reform.

It has been established in Chapter 5 that location data can become potentially sensitive depending on circumstances. In the light of the aforementioned developments it is important to offer ‘practicable’ privacy-respecting mobility pricing solutions that protect the anonymity of motorists. This study also explores whether economic constraints in shifting to anonymous solutions can be incentivised by asking for a dollar pledge from respondents to achieve this change. By means of a survey, this study seeks to incorporate public opinion in the design
process of privacy-aware telematics solutions.

The community is an important stakeholder, since all the data is being generated because of their movements. It is important to take their views on board and design solutions that are "community-ready". The results of this survey should provide a critical input in the design of privacy-aware telematics solutions from the consumers' perspective. Past surveys using psychological and experimental economics have focused on assessing the extent to which location information is valued by individuals (Acquisti & Grossklags, 2005; Cvrcek et al., 2006; Danezis et al., 2005), but have not sought user perception as an input to the design of privacy-aware models.

For mobility-priced insurance, the notion of "willingness to pay for privacy" has been explored. The survey aims to gauge a trade-off between privacy of location information and costs of setting up different privacy-respecting systems. Three possible alternative design solutions to mobility-pricing have been presented to respondents: full disclosure of GPS logs to insurance providers; aggregated information periodically sent to information providers; and no transfer of information to providers by conducting payment processing on-board the vehicle.

In tolling contexts "feasibility to pursue privacy" from a motorists' perspective has been explored in order to understand what issues have prompted the decline of anonymous options in the past. Is there a relation between convenience and privacy? The results of this survey could be used to predict which particular types of payment options would help in balancing privacy expectations and toll acceptance.

Section 6.2 reports the results of a preliminary online survey conducted to test these notions, followed by a detailed assessment of location experts in Section 6.3. The results of the second survey are discussed in Sections 6.4 - 6.6.
6.2 A Preliminary Survey of Online Attitudes

6.2.1 Instrumentation

The survey was made available online, and invitation emails to participate in the survey were sent to the School’s mailing lists for undergraduate students, postgraduate students, staff (academic and general) as well as to different privacy-based mailing lists, including the mailing list of Australian Privacy Foundation (APF)\(^1\) and Research Network for a Secure Australia (RNSA)\(^2\). The invitation email contained a brief description of the survey, and the web-site Uniform Resource Locator (URL) to the home page of the survey.

To reduce non-response and make the analysis and coding of survey data as simple as possible, closed-ended questions were used in the survey. The scale for all the variables was nominal (categorical), so only basic statistical operations could be performed (mode); even inferential statistics could only exploit the chi-square statistic.

6.2.2 Video Clip

The initial assumption was that participants had no information about telematics-driven payment systems, so a short animation was presented to them before taking the survey. Figure 6.1 illustrates some scenes from the animation that respondents watched. These scenes depict scenarios of the advantages of navigation and telematics systems; for instance how an emergency response can be dispatched in case of an accident/emergency, as well as scenarios demonstrating potential abuse of location information by third parties. It was expected that this animation would give potential respondents some idea of the operation of

---

\(^1\)APF is the primary non-governmental association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

\(^2\)RNSA is a multi-disciplinary collaboration established to strengthen Australia’s research capacity for Critical infrastructure protection (CIP) from natural or human caused disasters.
6.2.3 Questionnaire

Once the video clip ended, survey respondents were provided with a link to proceed to the questionnaire. Appendix A lists the survey questions. The respondents were asked to provide personal information including age, gender, profession, type of licence, and the type of vehicle they drive, in an effort to determine demographics for survey analysis. The null hypothesis postulated assumes that there would be no correlation between the choice that individuals made about privacy features and their demographics.

As shown in Appendix A, the ‘Telematics General’ section of the survey was designed to gauge the interest of respondents in acquiring GPS navigation.
devices for their vehicles, and to test if they had adequate understanding of its use.

The ‘Pay as you drive insurance and privacy’ section contained one of the most important questions of this survey, which was to probe respondents’ attitude in their choice when it comes to privacy-aware systems vs. costs of maintaining privacy. The idea here was to find out if users were keen on acquiring the highest level of privacy, regardless of the costs involved or moderately rated privacy threats, and wanted some measures of privacy control. In another question respondents were asked whether they would be interested in subscribing to loyalty programmes similar to credit card rewards, where location disclosure would be awarded with points that could be utilised to get discounts and gifts.

The ‘Social Relationships’ section explored location disclosure to social networks. Respondents were asked to reflect upon who they felt should access their location information during different times of the day, e.g., during working hours or after hours or on weekends.

6.2.4 Sample Space

A non-probability sampling technique known as ‘convenience modelling’ was used in this research, which means the survey is based on self-selection of respondents. With internet-based surveys, the common criticism is that they are not adequate for general population surveys. The criticism is well-founded, but this does not mean that internet survey results are of no value. A survey conducted by the Australian Bureau of Statistics (ABS) of adults with access to the internet in Australia concludes that web users are generally young, highly educated professionals (Australian Bureau of Statistics, 2000). It is acknowledged that the survey sample here is not truly representative of the wider community, but as telematics become widely available, and more people start using it, it is expected that their privacy preferences will closely match those of the sample population.
6. Methodological Assessment of User Perspective of Telematics

of this survey.

The data from this survey represents the opinions of 133 respondents, almost half of whom (49%) came from the 26 - 32 year age group. About 17% of the respondents did not drive a vehicle or have a licence to drive a vehicle. The participants were diverse with respect to profession, and the occupations ranged from business-men to engineers, but information technology professionals were over-represented at 54% of the sample. As mentioned earlier, the sample reaffirms that web users are mostly young professionals.

6.2.5 Key Findings

Telematics and GPS

In order to ascertain the importance of conducting privacy research in telematics, respondents were asked if they would be interested in acquiring GPS devices and telematics services for their vehicles. When asked if they would be interested in purchasing a satellite navigation product for their vehicle, 17% responded that they intended to purchase one in the near future, while 42% responded that they would buy one if the prices dropped significantly. While 26% said they were not interested in acquiring such a product in the near future, the rest said they were not interested at all. Therefore, more than half (60%) said they would consider buying a GPS navigation device sooner or later.

Similarly, when the respondents were asked if they would be interested in accessing telematics services, more than half (56%) responded that they would subscribe to freely available services, while 25% were even willing to subscribe to subscription-only services. This demonstrates that there is a potential market for telematics in the near future, as more than 81% of respondents were interested in telematics. Only 7% of the remaining respondents said they would not subscribe because of driver-distraction issues, while 11% responded that they were not interested in any telematics services. Therefore the perceived inter-
Privacy-aware Insurance Design

An important question of this survey is related to mobility-pricing and privacy. Respondents were given an explanation of GPS-based insurance and its potential benefits of increasing fairness for premium calculations. At the same time the survey also mentioned the potential threats related to location disclosure. Respondents were asked what option they would choose if new privacy preserving insurance products come on the market.

Figure 6.2 reveals that 11% of the surveyed population was willing to pay...
the highest infrastructure costs to maintain the top level of privacy. 28% were satisfied with moderate privacy options, and 12% wanted the cheapest premiums, even if it required them to disclose all location information. Other significant subgroups did not choose any form of GPS-based insurance because of privacy issues with such insurance (23%) or were satisfied with their existing insurance arrangements (19%).

Location disclosure to social networks

The last section of the survey aimed to ask respondents whom they would comfortably disclose their locations to at different times of the day. Four groups of people, namely, employers, peers, friends and family, and three types of time periods, namely, working hours, after hours, and weekends were identified. With regards to disclosure of location data to social networks, the majority of the respondents were agreeable to disclosing their location to family (or significant other) at all times (weekends, after-hours, working hours), whereas in the case of disclosure to friends the response was almost balanced, with a slight inclination towards willingness to disclose location to friends. More interestingly, the majority of respondents did not wish to reveal their whereabouts to associates from the workplace (both employers and peers).

Correlational analysis was performed to see whether there was a relation between respondents’ choice of the type of insurance option and disclosure to social networks. Bi-variate analysis between ‘people choosing a form of GPS-based (highest privacy, moderate privacy or lowest setup cost)’ and ‘location disclosure based on relationship and time’ reveals a significant relationship. There is a positive correlation (Pearson Chi-Square, significant at the 0.001 level) between these choices. In summary, what this means is that people who opt for any type of GPS-based insurance would most certainly only disclose their location to their families.
Demographics and rewards programs

Past survey based research has indicated that there is a relationship between demographics and the importance people place on their privacy (Westin, 1998). With the aim of verifying this finding, the survey asked respondents to provide demographic data, including age and gender, among other variables. Bi-variate analysis using Crosstabs in the Statistical Package for the Social Sciences (SPSS) led to a positive correlation between gender and subscription to rewards programs. There appears to be a relationship between the two (Chi-Square statistics significant at the 0.05 Level). Survey results suggest that the female populace is more wary of privacy abuse and values their privacy more, even if financial or other incentives like rewards programs are offered. The bar-chart in Figure 6.3 reveals that females censured incentives like rewards programs in exchange for location disclosure more than their male counterparts. This relationship is
consistent with Westin’s findings, which indicated a relationship between demographics and the level of online privacy concerns of respondents.

6.2.6 Conclusion

This preliminary survey confirmed that respondents valued their privacy and wanted finer control of release of their location information, as seen in their response to disclosure to social networks. Respondents were also willing to embrace mobility-priced insurance products which have some measures of privacy. For instance, Figure 6.2 shows that 28% wanted at least moderate privacy protection.

On the other hand, 42% of the respondents did not show interest in any of the mobility-priced insurance choices. This may be partly because of the fact that the question sought opinions on multiple issues. The question which listed choices of highest privacy to lowest privacy and also included non-interest due to satisfaction with current insurance or privacy reservations, is an example of a ‘multi-barrelled’ question. Multi-barrelled questions are generally discouraged in survey research, as they can introduce ambiguity and respondents’ perception of the question may change.

Additionally, all the questions were measured on a categorical scale, which does not tell much about the extent of agreement/disagreement with a statement.

The critique generated from this exercise played an important role in improving the design of the study conducted in Section 6.3.

6.3 A Detailed Assessment of Location Experts

From the findings of Section 6.2 it has been established that detailed information about ‘highest’, ‘moderate’ and ‘no privacy’ scenarios should be provided to respondents to enable an informed decision. In order to measure the changes in attitudes of respondents to the available options, it is best to present these
scenarios sequentially. It is not sufficient to only gauge whether respondents are interested in a particular product or not (yes, no). The intensity of their interest should also be measured to determine changes in perception. Similarly, the costs for each of these options should also be explored. Whether a respondent is willing to commit a higher pledge for setup costs of the highest privacy design should be measurable.

With regards to electronic tolls, the survey attempted to renew understanding of the user perspective of privacy threats of ETC, since the last survey in Australian contexts on tolls and privacy was taken at least a decade ago, as discussed in Chapter 4. It was also discussed that privacy concerns existed when electronic tolling applications were introduced almost two decades ago. As a result, some of them had to be discontinued, and some had to be retrofitted to introduce privacy respecting payment options. With the passage of time, these privacy-aware options became non-existent. It is possible that the popularity of anonymous payment options is to some extent dependent on its practical availability and the administrative burden imposed on those who might have otherwise wished to use it. This survey also attempted to answer the issues that may have led to the removal of privacy-features in past toll applications. Additionally, the NSW Government's decision to make a transition towards cashless tolling partially acted as a catalyst for this study to seek community opinion as to how this would impact their perceived notion of privacy. Because, as mentioned earlier, there was a portion of the population who were willing to forego the benefits of technology to preserve anonymity of movements.

6.3.1 Instrumentation

The survey instrument sought respondent attitudes on three themes, namely Telematics, GPS-based insurance and ETC.

Appendix B lists the questions comprising the survey. Questions that sought
a respondent’s agreement/disagreement are on an interval scale of 1-10.

There were instances of dichotomous variables, asking the respondents if they owned a GPS device, if they were aware of mobility-priced insurance, if they were aware of the decision that all roads in NSW would be tolled electronically, and which types of anonymous payment options they preferred.

There were also two questions that asked respondents to rate items in terms of importance, namely perceived accuracy of positioning technologies, and solutions for privacy-preservation.

For the amount willingly pledged by the respondent to cover setup costs, the response was on an ordinal (ordered) scale and values ranged from 'I want this device for free' to up to $1000. The survey also included some open-ended responses; these were put in to extract information about additional reasons when the response to a particular interval scale question was less than 5. Highest privacy was taken to be analogous to 'No GPS log disclosure/Computations onboard'; moderate privacy maps to 'Aggregate disclosure of GPS logs'; and no privacy concern was interpreted from to 'Full disclosure of GPS log'. The null hypothesis was that the median pledged amount would change as the respondent reads through the sequence of scenarios.

6.3.2 Sample Space

As the survey instrument evolved through several iterations of critique, it was clear that sample selection would be a critical aspect of this study. Most of the participants in the online survey belonged to the age group of 26-32 year old (49%) and had Information Technology (54%) as their profession. Such a sample space would be unsuitable to conduct an extensive study of privacy implications and a sample was required which offered diversity in terms of demographic characteristics, such as age, profession, type of vehicle owned, gender, education, earnings etc. and at the same time with a reasonable knowledge of positioning.
technologies to make informed decisions. For this reason, delegates at an International GNSS conference were selected as the target sample space. The delegates who attended included representatives from the European Unions' Galileo, the Russian GLONASS, GPS, Japanese QZSS, the US State Department, members from Australian government agencies, researchers and academics, as well as telematics and GPS industry personnel. Another reason for selecting this sample space for the research was that they would potentially be the opinion leaders in this field when it comes to design and policy consultations as they have a higher knowledge of the precision and operation of a multitude of positioning technologies as compared to members of the public. It was hypothesized that by following this approach, the opinions would provide a useful input to policy-making because of the inherent higher knowledge of these technologies that potential respondents would have as compared to the general public. The findings could still be extrapolated to the general population because of the diversity of the sample space.

As shown in Table 6.1, the age of these respondents was diverse, with 32% in the range of 21-30 years, 26% in the range of 31-40 years, 17% in the range of 41-50 years, and around 25% in the 51-60+ year range. This means that choices would reflect all age groups. Almost half (48%) of the respondents were graduates, while nearly 25% had postgraduate qualifications and nearly 20% had doctorates. With regards to seniority in their respective organisations, 39% belonged to front line management, 32% to middle management, and 26% held executive positions. Figure 6.4 summarises the distribution of respondents' professions. It can be seen here that various professions have representation here, including government, industry, research and academia.
Table 6.1: Demographic profile of respondents (N=78).

<table>
<thead>
<tr>
<th>Demographic Variable</th>
<th>Frequency</th>
<th>Percentage%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>28</td>
<td>36</td>
</tr>
<tr>
<td>Male</td>
<td>50</td>
<td>64</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-30</td>
<td>25</td>
<td>32</td>
</tr>
<tr>
<td>31-40</td>
<td>21</td>
<td>26</td>
</tr>
<tr>
<td>41-50</td>
<td>13</td>
<td>17</td>
</tr>
<tr>
<td>51-60</td>
<td>17</td>
<td>22</td>
</tr>
<tr>
<td>60+</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAFE</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Diploma/Certificate</td>
<td>3</td>
<td>3.8</td>
</tr>
<tr>
<td>Bachelors Degree</td>
<td>38</td>
<td>48.7</td>
</tr>
<tr>
<td>Postgraduate Diploma</td>
<td>8</td>
<td>10.3</td>
</tr>
<tr>
<td>Masters Degree</td>
<td>12</td>
<td>15.4</td>
</tr>
<tr>
<td>Doctorate</td>
<td>16</td>
<td>20.5</td>
</tr>
<tr>
<td><strong>Authority</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Front Line Managers</td>
<td>31</td>
<td>39</td>
</tr>
<tr>
<td>Middle Management</td>
<td>25</td>
<td>32</td>
</tr>
<tr>
<td>Executive positions</td>
<td>21</td>
<td>26</td>
</tr>
</tbody>
</table>

6.3.3 Data Collection

A self-administered questionnaire was distributed in print format to the conference delegates on the third day of the conference. On the 2nd day an interesting panel session had discussed location privacy and policy issues with regards to location based service. It was decided that the best time to get maximum responses would be after panel sessions, as the delegates would have a better appreciation of this exercise.

As shown in Appendix B, the cover page listed the key terms used and explained to the participants that they had been chosen to participate because of their ‘knowledge and interest in Geo-Information’, and the findings of this research would help in designing privacy-aware transport telematics.
6. Methodological Assessment of User Perspective of Telematics 163

Figure 6.4: Distribution of respondents’ profession.

6.3.4 Analysis

A total of 246 persons had registered to attend the three day conference. It is estimated that 95 participants were present on the last day of the conference. A total of 78 valid survey responses were collected, yielding a response rate of 82%. Survey analysis involved the generation of a code-book for the responses and variables, followed by data entry, and error checking for inconsistent and out-of-range variables. Responses to open-ended questions were entered onto a spreadsheet, and similar responses were used to create new categories. The statistical package SPSS was used for conducting statistical tests on the data.

The first step in statistical processing of this data was ‘descriptive analyses’ of the different survey questions to see the central tendency of their distributions. As most of the variables could at least be considered on an ordinal scale, statistical median was the preferred measure of central tendency for this study; although the mean was also considered in some cases where the variable could
be measured on an interval scale. For some charts where boxplots were used, the median, the interquartile range, the outliers and extreme values were displayed. The second step was to perform 'relational analysis' to see whether any two variables were correlated to each other. Survey research has previously yielded interesting correlations between demographics and the object of study, so the aim here was to find whether any demographic features caused any significant change in behaviour or not. The final step was to perform 'significance testing' to see whether the findings of the survey were merely by chance or were of statistical significance.
Table 6.2: Respondents ranking of technologies for privacy-invasiveness

<table>
<thead>
<tr>
<th>Ranks</th>
<th>GPS Logs</th>
<th>Electronic Tolls</th>
<th>Mobile Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>47</td>
<td>20</td>
<td>11</td>
</tr>
<tr>
<td>2nd</td>
<td>25</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>3rd</td>
<td>1</td>
<td>32</td>
<td>38</td>
</tr>
<tr>
<td>Total</td>
<td>73</td>
<td>73</td>
<td>73</td>
</tr>
<tr>
<td>Missing</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>N</td>
<td>78</td>
<td>78</td>
<td>78</td>
</tr>
</tbody>
</table>

6.4 Principal Findings for Telematics

6.4.1 Respondents’ Awareness/Interest in Telematics

Figure 6.5 summarises the distribution of familiarity with telematics services, the interest in telematics services and the interest in buying a GPS product. The first column on the boxplot indicates a median familiarity of 2, whereas the extreme values go up to 7-10 and are in a minority. On the contrary, the great majority of respondents were interested in subscribing to telematics services as they become available. The median interest in subscription was 5, the interquartile range was from 3-7, while the whiskers went up to the highest value of 10. When respondents were asked about their interest in purchasing a GPS navigation product, the median was even higher than that in telematics subscription, at 6, and the interquartile range was also higher and ranged from 4-8. These results indicate that GPS ubiquity in vehicles would pave the way for telematics service availability.

6.4.2 Perceived Threat of Telematics Technologies

Respondents were asked to rate the available location identification technologies, namely GPS logs, electronic toll collection records, and mobile phone based positioning, in terms of their precision to store movement data. As shown in Table
6.2. participants overwhelmingly rated GPS data as the most invasive tracking technology available, with toll records ranked second and mobile phone positioning ranked third. A 2nd rank analysis also revealed that GPS logs had the highest responses for invasiveness, followed by mobile phones and toll collection records. Interestingly, it can be observed that the combined 1st and 2nd ranks for GPS and tolls are 72 and 41, respectively, which is higher than the combined 1st and 2nd rank for mobile phones (35). This means that respondents felt more threatened by toll records, probably because they at least had the option of switching their mobile phones off to avoid tracking, while toll tags, whether removed or kept intact, would record a vehicle’s movements at toll gantries (presumably thorough ANPR).

When respondents were asked to rate the statement, ‘people may be tracked using telematics and GPS technologies’ on a scale of 1-10, and also to express their concern about ‘secondary uses of location information’, Figure 6.6 demonstrates that participants were more threatened by tracking of their vehicles than by secondary usages of their stored location data. The median threat perceived on a scale of 1-10 for tracking was 7, and majority responses were contained within a high range of 5-8, compared to the median for secondary uses (6) and an interquartile range of 4-8.

6.4.3 Privacy Remedies

Table 6.3 summarises participants’ responses with regards to effective solutions for location privacy. More than 56% of the respondents agreed that privacy-respecting technologies were the number one solution for spatial privacy issues. About 32% of respondents selected targeted legislation as the highest safeguard for privacy, while 10% felt privacy policies could protect against privacy abuses, and only 4% rated industry codes of practice to be the solution. It can be observed from the counts for Rank 1 and Rank 2, that privacy-aware design
Figure 6.6: Boxplot representing distribution of perceived threats of telematics and secondary uses of data.

Coupled with targeted legislation were perceived to be the two most important tools for managing privacy issues in the locational arena.

6.5 Principal Findings for ETC

6.5.1 Awareness of and Concerns about Tolling

Table 6.4 summarises respondents' knowledge about the legislation aimed at achieving state-wide (NSW) electronic tolling. Almost 60% of the respondents were aware of this decision. Further, Figure 6.7 represents the perceived threats respondents felt from the tracking of individuals using tolls and from secondary
Table 6.3: Respondents’ ranking of privacy solutions in terms of effectiveness

<table>
<thead>
<tr>
<th>Ranks</th>
<th>Solution</th>
<th>Privacy-respecting Technologies</th>
<th>Targeted Legislation</th>
<th>Privacy Policies</th>
<th>Industry Codes of Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td></td>
<td>40</td>
<td>23</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>2nd</td>
<td></td>
<td>16</td>
<td>30</td>
<td>17</td>
<td>7</td>
</tr>
<tr>
<td>3rd</td>
<td></td>
<td>7</td>
<td>11</td>
<td>31</td>
<td>22</td>
</tr>
<tr>
<td>4th</td>
<td></td>
<td>8</td>
<td>7</td>
<td>16</td>
<td>38</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>71</td>
<td>71</td>
<td>71</td>
<td>70</td>
</tr>
<tr>
<td>Missing</td>
<td></td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>N</td>
<td></td>
<td>78</td>
<td>78</td>
<td>78</td>
<td>78</td>
</tr>
</tbody>
</table>

Figure 6.7: Respondents’ perceived threat of tracking and secondary uses of toll data.
6. Methodological Assessment of User Perspective of Telematics 169

Table 6.4: Awareness of fully electronic tolling decision in NSW

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>46</td>
<td>59</td>
</tr>
<tr>
<td>No</td>
<td>32</td>
<td>41</td>
</tr>
<tr>
<td>Total</td>
<td>78</td>
<td>100</td>
</tr>
<tr>
<td>Missing</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>N</td>
<td>78</td>
<td>100</td>
</tr>
</tbody>
</table>

uses of ETC data. Responses to these questions were on a scale of 1-10, where higher numbers represent a higher perceived intensity of threats. The dark lines in the middle of the box-plots indicate the statistical median (or 50th percentile), while the lines enclosing the rectangles indicate inter-quartile ranges (25th and 75th percentile). Respondents' perceived threat from tracking gave a median value of 7, as compared to the median value of 5 for secondary uses. This means that respondents were more concerned about the real-time surveillance that tolls enabled than about the secondary uses that this data can be used for.

Table 6.5: Perceived threats to privacy

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Tracking</th>
<th>Secondary Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>N Valid</td>
<td>76</td>
<td>76</td>
</tr>
<tr>
<td>Missing</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Mean</td>
<td>6.47</td>
<td>5.59</td>
</tr>
<tr>
<td>Std. Error of Mean</td>
<td>.282</td>
<td>.275</td>
</tr>
<tr>
<td>Median</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Std. Deviation</td>
<td>2.46</td>
<td>2.4</td>
</tr>
</tbody>
</table>

A close analysis given in Table 6.5 shows that the mean values of threat from surveillance and threat from secondary uses are 6.47 and 5.59 respectively. While the mean is slightly lower than the median values here, the difference in their values suggests that the same observation still stands.
6.5.2 Inclination Towards Post-Paid Anonymity

This section measured respondents' interest in an electronic tolling system which works anonymously. On a scale of 1-10, respondents were asked to indicate a number that best described their interest in such a system. Considering Figure 6.8, if a score of 7 and above is assumed as a response indicating high interest, nearly 66% of the respondents said they were highly interested in embracing an anonymous electronic tolling solution.
Table 6.6: Perceived interest in an anonymous cashless tolling system

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Interest in anonymous and cashless system</th>
</tr>
</thead>
<tbody>
<tr>
<td>N Valid</td>
<td>76</td>
</tr>
<tr>
<td>Missing</td>
<td>2</td>
</tr>
<tr>
<td>Mean</td>
<td>6.93</td>
</tr>
<tr>
<td>Std. Error of Mean</td>
<td>0.282</td>
</tr>
<tr>
<td>Median</td>
<td>7.5</td>
</tr>
<tr>
<td>Std. Deviation</td>
<td>2.446</td>
</tr>
</tbody>
</table>

Table 6.6 shows the mean and median values for their interest, which are 6.9 and 7.5 respectively. Although the mean is slightly lower than the median in this case, the values still represent a strong sign of respondents' inclination to such a system. Westin (1991) classified online privacy attitudes into those of the fundamentalist minority, pragmatist majority and the marginally concerned. Consistent with his research, a similar trend can be observed in this sample too, as summarised in Figure 6.9. There is a presence of the marginally concerned (scale of 1-5) constituting 23.68% of the responses, followed by the privacy pragmatists (scales 6-8) comprising of 47.37%, and a fundamentalist minority (scales 9-10) of 28.95%.

When the respondents were asked to give their preferences about settling payments for this anonymous tolling scheme (Figure 6.10), 36.5% chose pre-payment, while an overwhelming majority of 63.5% desired post-payment of tolls on anonymously tolled roads. This proved to be one of the key outputs of this survey, as one of the issues that had been observed in Section 4.3.9 was that privacy-respecting features that were made available in past applications often did not attract significant attention, leading to a gradual phasing-out of such options.
6.5.3 Demographics and Payment Choices

Relational analysis of gender, payment options and interest in anonymous tolling shows that both men and women who expressed a higher interest in anonymous tolling also preferred postpaid arrangements. Secondly, consistent with past research about privacy attitudes and demographics (Westin, 1998), this study reaffirms that gender and privacy attitudes are related. As shown in Figure 6.11, women tended to display a higher interest in privacy technologies than their male counterparts. For respondents who preferred post-paid options, their interest in anonymous tolling tended to be concentrated in the range of 5-10 for men and 6-10 for women, with median values of 7.5 and 8 respectively. On the other hand, the interest in anonymous tolling of the remaining 35% of the respondents who preferred pre-payment ranged from 1-10 for men and 6-8 for women (a smaller subgroup) with median values of 5 and 7 respectively. To summarise, it can be said that the majority of participants were interested in anonymous
tolling options and had a preference for paying their tolls post-paid, as in existing identifiable cashless tolling. Technically this looks like a real challenge, where respondents prefer anonymity without being disadvantaged by having to buy pre-paid credit, which they may or may not use in the near future. Section 7.3 discusses the technological possibilities of 'postpaid anonymity' of tolls.

Exploring the prospect of whether the age of respondents caused any significant inclination towards anonymous tolling or payment options revealed some interesting findings. There appears to be a correlation between the age of respondents, the type of payment chosen, and inclination towards anonymous tolling. Figure 6.12 shows that the age group of 21-30 and 31-40 had a higher inclination towards anonymous tolling. When it comes to the type of payment, these same subgroups preferred post-paid payments, with median interest values of 8 for the subgroup 21-30 and 7.5 for the subgroup 31-40, respectively. Statistics from

Figure 6.10: Respondents' opinion on pre-pay vs. post-pay anonymity.
Figure 6.11: Box-plot showing relationship amongst payment type, gender and interest in anonymity.

The 2006 census of Australia reveals that 29% of all Australians fall within the age range of 21-40 (Australian Bureau of Statistics, 2006); therefore the views of this population subgroup are important in shaping future privacy-aware tolling practices and redressing the imbalance of technology and privacy on roads.

6.6 Principal Findings for GPS-Enabled Insurance

6.6.1 Privacy-Aware Insurance Scenarios

This section of the survey sought respondents’ opinions on and interest in three types of mobility-priced insurance products as well as their level of willing price
pledges to cover setup-costs for each of these. The survey description explained to respondents that all three types of these products would give similar cost savings compared to traditional insurance premiums, but that the way these designs are implemented would require changes or alterations to telematics boxes and computing and could require a pledge of support from those patrons who were willing to pay for higher privacy protection of their locational attributes.

The distribution of pledged amounts can be observed from Table 6.7. The pledge choices start from zero and go up to a thousand dollars. It can be observed that the number of respondents preferring no payment for full disclosure has been reduced by 14 (about 18% of the sample space) in the case of aggregate disclosure. The number of participants who opted for no payment was further reduced in the case of no disclosure (highest privacy) option. These numbers

Figure 6.12: Boxplot showing relationship amongst age, payment type and interest in anonymity.
suggest that there was a change in perception, and that participants pledged actual amounts for aggregate and non-disclosure. Observing the row for $100 pledges reveals that the pragmatist majority opted for a moderate measure of privacy. The row for $250 pledges shows that the pragmatist and fundamentalist pledges are same in number. However, the pragmatist majority is overtaken by the fundamentalist minority for pledges of $500 and $1000 respectively.

The variation in pledged amounts over the three scenarios may be a step towards affirming the initial hypothesized behaviour of participants adjusting their interests and pledges on the basis of the choices provided. Figure 6.13 represents the distribution of pledged amount over the three options. Ignoring responses of zero dollar pledges, the median bid for full disclosure is $100, whereas it is $250 for aggregate and no disclosure respectively. The whisker for the no disclosure boxplot reaches $1000 for a single fundamentalist pledge made to receive the highest protection. To test whether these values are statistically significant, a pair-wise t-test was conducted between full disclosure and moderate disclosure, moderate disclosure and no disclosure respectively, assuming these quantities to be on an interval scale. Paired sample correlation between full disclosure and moderate disclosure is quite strong (0.596), while for moderate disclosure and no disclosure it is a little less significant (0.437). The paired sample t-test indicates
that there is some merit in the significance of these correlations and that they are not merely by chance, thus confirming the initial hypothesis.

6.6.2 Correlation of Privacy Choices and Demographics

The online study indicated that demographics may prove significant when choices about privacy protection are made. Previous studies have also verified this notion (Westin, 1998; Huberman, Adar, & Fine, 2005). Taking these variables into account, the survey instrument collected demographic information of the participants. Correlation analysis between demographics and pledges/interest was performed. The results are discussed below.

Figure 6.14 is a boxplot of the relation between the type of vehicle a participant owned and the distribution of interest in the three designs. It can be observed that small car and four-wheel-drive owners are distributed 'pragmatically', where moderate disclosure has a higher median value compared to
full disclosure and no disclosure. In the case of family car owners, the median interest for full disclosure and moderate disclosure is the same, but the interquartile range for full disclosure is greater, suggesting that family car owners may prefer savings over privacy. Quite interestingly, sports car owners expressed a considerably high interest (median of 9) in the no disclosure (computations on-board) option, possibly to protect themselves from embarrassing circumstances where the insurer could be able to find about the speed capabilities of the vehicle in general, or specifically, when insurance claims are filed. With the exception of extreme values, luxury car owners seemed indifferent to the three types of cost/privacy trade-offs. In fact when the reasons for the lack of interest were probed further for luxury car owners, the majority of them cited that they were happy with their current insurance arrangements.

The preliminary study suggested that women were more suspicious about loyalty programs than men which is consistent with past research on correlation between gender and the wish for privacy (Westin, 1991). A relational analy-
sis between gender and distribution of pledges for the 3 designs was performed. Figure 6.15 illustrates a boxplot of the pledge distributions over gender, indicating that the female populace pledged a higher median amount ($250) for no disclosure (highest privacy) than for moderate and full disclosures ($100).

Exploring the demographic of age for correlations led to further interesting findings. The boxplot graph in Figure 6.16 shows pledge distribution with respect to the age range of participants. It can be observed from this graph that the subgroup of participants aged 20-40 (21-30, 31-40) valued moderate and no disclosure more highly than cost savings at setup. Their notion of choosing some privacy of location information may be attributed to the fact that young adults are more cautious about revealing personal data, or have more to hide than older people.
6.6.3 Qualitative Analysis

Question 3, 6, and 9 in Section B of Appendix B asked respondents their reason for lack of interest when they provided a number from 1-5 for the question related to their interest in the three designs respectively. This section analyzes the open-ended responses of the participants in an effort to study what circumstances prompted their attitude. Table 6.8 lists some of the significant responses exactly as written by the participants.

It is evident that there is a lot of concern about potentially surveillance-enabling (full disclosure) one’s vehicle by installing such systems. This perception is also echoed in one of the participant’s opinions: ‘Do not want vehicle tracked!’. Others highlighted the legal implications of surrendering all the location profiles to a central server, where it would possibly be stored indefinitely and could be used in legal circumstances as evidence against the insured person.
Table 6.8: Respondents reason for disinterest in the 3 design choices.

<table>
<thead>
<tr>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
</tr>
<tr>
<td>R2</td>
</tr>
<tr>
<td>R3</td>
</tr>
<tr>
<td>R4</td>
</tr>
</tbody>
</table>

Another participant said ‘Insurance companies operate for their benefits more than ours!’

For moderate and no disclosure some participants identified that having no access to the vehicle’s precise movements would restrict dispatch of telematics-enabled emergency response, for instance in case of an accident. Another significant point highlighted by a few of the respondents was that no-disclosure systems could be prone to cheating, as there was no independent mechanism to verify whether the payments were being calculated correctly on the vehicle. Most of the uninterested participants shared a common sentiment of suspicion against insurance providers across all the three designs, indicating that they did not trust insurance companies, and that consumers would have to bear the cost of any modifications when transitioning from classical insurance arrangements to mobility-priced ones.
6.7 Summary

The survey confirmed that respondents were interested in acquiring GPS and telematics devices, but at the same time felt threatened by their real time tracking capabilities.

Survey results indicate that while GPS-enabled logging had the highest perceived precision, respondents felt that electronic tolls posed a higher threat than mobile phone based localization, probably because people have the choice to switch off their mobile phones when they want to avoid tracking, but electronic tolls would still digitize movements whether a toll tag is activated or not.

The mean values for the fear of threat from secondary storage of data were less than those for the threats from tracking, possibly because the respondents underestimated the real threats of retention and function creep. In actuality, the threats from secondary uses are equally perilous when privacy, mobility and data-mining are considered in the same scenario.

The survey results also suggest that motorists do not want to be disadvantaged in choosing the type of payment options if they have a higher appreciation for privacy. They want similar options for payment of toll charges available to other electronic toll consumers.

The majority of respondents were interested in mobility pricing and did not expect absolute privacy guarantees. While privacy expectation was not particularly high for the majority pragmatists, there was a reasonable expectation of being able to control the granularity and disclosure of that information. It is also clear that users valued their social relationships strongly when it comes to location disclosure. There was a tendency to disclose personal location information to only close family members.

Qualitative analysis also highlighted important issues, such as what are the legal implications for the patron who discloses all the locational data to the insurer? Does a situation of no privacy, no setup cost mean that the patron has
no say in how the data about his/her movements is used? How secure would the on-board computation model be to cheating? How can it be independently verified that the system’s payment equations are not over-charging the motorist?

All these issues highlight that there is a critical need to recalibrate information practices by developing privacy-respecting technology solutions which provide similar services with minimal impact on consumers’ privacy. The need for this shift is also highlighted in the survey results, wherein more than half of the respondents thought that privacy-respecting technology was one of the most important ways of achieving this balance.
Chapter 7

User-Perception Inspired Privacy-Aware Models

7.1 Introduction

Privacy-aware pricing of GPS-based insurance is presented in Section 7.2. GPS-based pricing is a passive system logging all movements and periodically transmitting them to a server for premium processing. The spatial resolution is high, with precise movement details collected. The motorist has a choice in adopting this class of insurance, as it is not mandatory for vehicle insurance to be priced using distance. However, even anonymous GPS data can be used to make inferences about people.

A solution to anonymous toll collection is presented in Section 7.3. ETC has gradually been established in the last twenty years and mostly uses RFID for identifying vehicles. It is inherently an active system, with a resolution depending on the density of the toll network. This system records the passage of all registered vehicles for revenue collection, and photographs all vehicles passing toll gantries. Survey results suggest that post-paid anonymity is desirable for motorists.
7.2 Privacy-Aware GPS-Enabled Insurance

In the context of GPS-based insurance, the location of a vehicle is used to provide a customised insurance product aimed at actuarial accuracy and fairness for the motorists. Sections 7.2.1- 7.2.3 revisit some of the critical issues established in Chapters 4, 5 & 6 as a result of server-based personalization approaches whose privacy threats outweigh the promised benefits to the motorists. These recommendations serve as critical inputs to the privacy-aware pricing model presented in Section 7.2.4.

Existing implementations of mobility-priced insurance designs have been reviewed in Section 2.5.2. All GPS-based insurance designs are highly invasive of motorists' privacy. That said, GPS-based designs have the potential to be a more accurate reflection of risks faced by motorists by using the 'where' and 'when' to design insurance premiums based on those risks, which would be fairer than the traditional methods.

7.2.1 Results for Insurance from the Analytical Framework

The analytical framework presented in Chapter 4 identified that GPS-enabled processing would constitute a passive system which provides precise and detailed movement records of the motorist. The problem with such a passive system is that it silently logs and transmits all movement data with the premise of using it for generating premiums. The motorist cannot control the granularity of the information released, since data of the highest accuracy and resolution is collected and transmitted periodically, without input or intervention, and is stored in a database for processing premiums, but could possibly be used for purposes never intended when this data was collected.

Even though a motorist has a choice of not signing up for mobility-priced
insurance because of privacy concerns, this means they cannot reap the benefits of an accurate and fair insurance policy, which could have possibly brought premium savings. On the other hand, if a motorist signs up for existing mobility-priced insurance schemes, they lose the right to anonymous travel, and would have to disclose all movement data for insured driving. In summary, the data is a collection of spatio-temporal footprints of the motorists' movements revealing that a motorist was at a location \( X \) at a time \( T \), which is a lot more detailed information than the desired total distance on different roads.

### 7.2.2 Results on GPS-based Insurance from the Threat Model

The problem reviewed in 7.2.1 is a result of the possible association between the identity of the motorist and their movements. It has also been demonstrated in Chapter 5 that the privacy of the motorist is not sufficiently protected even if the provider starts storing data 'anonymously' after processing premiums. The nature of high resolution GPS data is such that it can be used to launch inference attacks, to infer the 'identities' of the motorists, on the basis of their pattern of movements, and to render anonymous storage ineffective. These scenarios substantiate the proposal that data should be processed in-vehicle and only the aggregate be sent to the provider as a notification.

### 7.2.3 Survey Results on Privacy-aware Insurance

This section revisits the survey results presented in Chapter 6 with a view to incorporating important recommendations into the design of the model proposed in this Chapter.

More than half of the respondents (56\%) had agreed that privacy-aware technical solutions were the best approach to handle privacy issues in telematics applications. This acted as a catalyst to look for alternate designs for mobility
pricing with privacy-embedded features.

Results from the survey also suggest that respondents were interested in mobility-pricing's potential saving incentives, but at the same time were not prepared to relinquish their right to privacy. The majority of motorists held a pragmatist opinion towards preserving privacy and were prepared to pledge a dollar amount for privacy-respecting solutions, the median value being AUD 100 for systems that aggregated data via a payment equation on-board and only sent the total distance and the total premium amount back to the insurer.

Respondents were comfortable with revealing their location information to their respective partners only. At the same time, qualitative analysis revealed that respondents thought that systems that aggregated information in-vehicle were not capable of being used in emergency response situations for notifications.

Survey results also suggest that respondents were skeptical about the audit mechanisms of closed systems (aggregate data transmission, and no transmission). How would it be possible to verify that the premium processing equation is functioning accurately? How could it be verified that the motorist is not deceiving the system by under-estimating the trips taken? These questions led to critical analysis of these issues and helped refine the design of a privacy-aware mobility-pricing system.

### 7.2.4 Conceptual Design

The aim of this research is to demonstrate that it is possible to design privacy-sensitive GPS-based insurance products that keep motorists' freedom of movement intact without affecting the level of service. Current data exchange, storage and retention practices, which have the possibility of revealing a great deal more about motorists, are a cause of increased privacy sensitivities from a motorist's perspective. It is important to recognise and respect the driver's location privacy concerns if the insurance industry wants GPS-based insurance to be a suc-
cessful business model. In light of the aforementioned recommendations a design is proposed that aims to assuage the tension between the competing interests of the privacy of motorists and collection for accurate revenue processing.

It was discussed in Chapter 4 that despite privacy concerns GPS-enabled systems offer by far the greatest flexibilities to policy designers. If a self-positioning system such as GPS also becomes a self-payment system by calculating premiums on-board, the flexibility to offer variable risks-based insurance that preserves privacy becomes viable. As automobiles evolve from mechanical systems to a set of many computer-assisted subsystems, implementing an on-board solution becomes even more probable. It is possible to use the on-board computer to perform the tasks that were previously done by the insurance provider’s central server since vehicles are evolving into mobile computing environments. The design proposed here is very similar to current GPS-based insurance architectures, except for the fact that there is an OBE installed in the vehicle which encapsulates the role of the central processing server and analyzes the GPS records to calculate the distance, which roads the vehicle was driven on, what times of the day and under what conditions, in order to estimate premium per kilometre. Figure 7.1 illustrates the difference between the current GPS-based implementations and the proposed privacy-aware design.

The proposed design also takes into account other factors affecting motorists’ risk on roads. Road conditions are assessed using sensory input attached to the vehicle, such as humidity and light sensors. The insurer provides a payment equation which computes risk per kilometre in real-time, based on the inputs obtained from the GPS receiver and other sensors. The system also uses the combination of speed limits and current speed to vary risk, and indicates to the motorist via a visual interface that higher risk is being taken. This would also encourage the motorist to minimize risk (and premiums) by employing speed adaptation. It is believed that using these sensors and GPS data to compute
premiums per kilometre would be a true reflection of the risks faced by a motorist on the road. The design provides two choices for premium payments: firstly, pre-paid, by implementing an on-board anonymous payment system by means of prepay-smart cards, and secondly post-paid, by transmitting the amount to be debited via SMS to the insurance provider. The OBE can provide irrefutable evidence of payments on random system audits. At the time of policy setup, the motorist may nominate a person to be notified of their location in case of an emergency. An emergency signal would be activated when the car undergoes a crash. Since, the insurance provider’s interest is in receiving accurately charged premium payments, it would not be concerned with monitoring the movements of motorists. The output is a privacy-friendly design that eases the tension between the interests of insurer and insured.
7.2.5 Description

Hardware

The hardware used in the system is assumed to be tamper-proof, including the GPS receiver, the humidity sensors and light sensors. The specific equation that calculates the premium is provided by the insurance provider, along with a spatial map of the road network and a spatial database of risks and speed limits for roads. The OBE consolidates the inputs received in real-time (GPS, sensory input) and matches those to the other inputs (speed limits, road risks) and loads them into the payment equation as shown in Figure 7.2.

Distance vs. Speed

While proponents of distance-based charging have long advocated the benefits of potential reduction in accident claims and the fairness of these systems (Litman, 2003), there is another school of thought which claims that speed plays the most critical part in road safety. In road transport systems legislation puts the onus on motorists to observe speed limits on roads for their and other road-users' safety. Real speed and accident statistics, however, show that safety is not the highest priority for motorists. Compliance with speed limits is low and the average speed limits are higher than the set speed limits on almost all types of roads (Várhelyi, 1996). Various trials have been conducted on Intelligent Speed Adaptation (ISA) and have demonstrated significant accident savings and community benefits (Almqvist, Hydén, & Risser, 1991). ISA systems continuously monitor the current speed and map that to the speed limit by using a combination of spatial maps and GPS. These systems then either alert the motorist of over-speeding (passive ISA) or support them to slow down (active ISA) such as by means of an Active Accelerator Pedal (AAP) (Hjälmdahl, Almqvist, & Várhelyi, 2002).

The offering of discounts on insurance for motorists installing ISA systems
Figure 7.2: Schematic representation of the Privacy-aware GPS-enabled insurance model.
has already started emerging. Lindberg, Hultkranz, Nilsson, et Thomas (2005) reported two economic field experiments that tested ways to influence motorists to install devices in their vehicles which incentivized them on insurance premiums for observing speed limits. Their study concluded that offering insurance discounts for motorists installing ISA would lead to motorists' acceptance of the technology. They also concluded that the economic share of the bonus should be made dependent on the actual frequency of speeding. For instance, a pilot study in Denmark in collaboration with an insurance provider offers discounts of up to 30% in insurance premiums using ISA systems (Agerholm, Waagepetersen, Tradisauskas, Harms, & Lahrmann, 2008). This system notifies the motorist if they speed and applies penalty points that lead to a decrease in discounts if the motorist does not observe speed limits.

Since ISA systems also use GPS and spatial maps of road speed data, it is possible to achieve the benefits of both GPS-enabled insurance and ISA by combining the two systems. This design chooses passive ISA, since it would be available with minimum installation efforts. The privacy-aware GPS-enabled insurance system would take current speed as a risk and include that into calculating premiums. At the same time it would also act as a passive ISA system, reminding/encouraging the insured to slow down. Variable insurance costs would be an incentive to use speed alerts for saving on premiums. Since the proposed system would use speed as part of costing insurance premiums, the ISA system could either be pre-installed, offering further opportunities of savings, or be sold as an add-on application for additional savings on insurance by encouraging a change in behavior. Besides, in a broader context, a proactive approach such as an ISA system would help encourage the motorist to become a safer driver in the long run and reduce the need for installing speed enforcement cameras which are inherently reactive and privacy-invasive.
Table 7.1: A possible catalogue of weather conditions & associated risk.

<table>
<thead>
<tr>
<th>Weather Conditions</th>
<th>Associated Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dry</td>
<td>1</td>
</tr>
<tr>
<td>Light Rain</td>
<td>2</td>
</tr>
<tr>
<td>Moderate Rain</td>
<td>3</td>
</tr>
<tr>
<td>Heavy Rain</td>
<td>4</td>
</tr>
<tr>
<td>Light Freezing Rain</td>
<td>5</td>
</tr>
<tr>
<td>Moderate Freezing Rain</td>
<td>6</td>
</tr>
<tr>
<td>Heavy Freezing Rain</td>
<td>7</td>
</tr>
<tr>
<td>Light Snow</td>
<td>8</td>
</tr>
<tr>
<td>Moderate Snow</td>
<td>9</td>
</tr>
<tr>
<td>Heavy Snow</td>
<td>10</td>
</tr>
</tbody>
</table>

Pay How You Drive

Automobile manufacturers are fitting new cars with various sensors to improve their safety and reliability. For instance, there are light sensors widely available that activate headlight lamps at dusk or in darker conditions. Likewise, humidity sensors activate windscreen wipers if they sense moisture on the windscreen (BMW Australia, 2008; Hyundai Azera, 2008; RainTracker, 2008). There are also rear and front parking sensors that help in determining the distance from the front and rear vehicle when parking. All these sensors can be used to assess road conditions and hence measure the risks that a motorist faces in real driving conditions. Research suggests that driving in wet and dark conditions is more risky than driving under normal conditions (Litman, 2005). Besides these sensors, the speedometer reports the driven speed continuously. To authenticate speed, the GPS receiver is also capable of estimating the speed of the vehicle by simply taking two successive GPS positions in time. This could possibly be used to identify speedometer tampering.

At the time of setting up a policy, the insurance provider collects basic information such as driving experience, claims history, age, sex, residential address, garaging location, year and make of vehicle, price insured for, security equipment
fitted to the vehicle and any alterations made to the vehicle. This information could 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 thesis, and is better addressed in actuarial science, but it is assumed here that a premium payment equation would be provided by the insurance provider, which would be plugged in to the vehicle’s OBE to perform premium calculations in real-time.

The light and weather sensors report the light (dark or light) and weather (wet or dry) conditions to the OBE for processing. Since these sensors gather input from their surroundings, this analogue data would be converted to digital format before reporting to the OBE. There is a related risk table that is looked up to select a risk value for the reported light (Table 7.1) or weather variables (Table 7.2). The light or weather sensors interact via a communications channel [wired or wireless (infrared or Bluetooth)] with the OBE reporting a numeric value. The OBE computes Weather Conditions Risk (WCR) and Light Conditions Risk (LCR) by exponentiating these values and plugs them into the premium processing equation as shown in Equation 7.1.

\[
\frac{\text{Premium}}{\text{KM}} = \text{BaseRate} \times WCR \times LCR \times RHR \times SR \times RR
\]  

(7.1)
Where,

- Base Rate = Depends on gender, age, experience, etc.
- WCR = Weather conditions risk
- LCR = Light conditions risk
- RHR = Rush hour risk
- SR = Speeding risk
- RR = Road risk

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 located 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 current 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 from research related to accidents and high risk neighborhoods. This particular risk is computed as Road Risk (RR).

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). The OBE exponentiates these risk values (depending on the payment equation) and then loads them into the payment equation to calculate the premiums per kilometre.

**Payment Options**

**Post-paid payment system**

In this payment method, the premium per kilometre is aggregated over the
month and the total value along with the total distance is sent to the insurance provider via an SMS message. The insurance provider uses this information, and generates an invoice which is mailed to the insured for payment. In this method of payment the insured reveals the monthly spent amount to the insurance provider. Since this is a periodic payment arrangement, the insured is implicitly covered between successive billing cycles during the contract period.

Anonymous payment system

Digital cash or e-cash has been a prevalent concept in 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 anonymous payment system, however, uses anonymous digital payment to completely preserve the privacy of the payment habits of an individual for insurance. This payment system offers 'privacy of spending', and is at a higher level than post-paid systems. The anonymous payment system uses blind signatures first proposed by Chaum et al. (1990). This approach has been used efficiently in electronic payment systems, and preserves the identity of individuals making transactions.

If the insured wants a closed system, as discussed in the three choices given to survey respondents in Chapter 6, and is inclined towards not disclosing spending habits to the insurer, an anonymous payment option can be used. 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 to the of topping up of prepaid mobile phones or phone cards. This smart card would have the aforementioned anonymous qualities of cash, i.e. secure and untraceable cash. These smart cards would be available to the individual from a pool of new smart cards. They would not require identification of the individual; therefore, the identity of the individual could not be ascertained from them. The smart card can be inserted
into a card reader on the vehicle's OBE. 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 remind the insured individual to recharge the card to gain insurance, similar to a fuel warning indicator.

The OBE could keep track of when the vehicle was used without insurance and could possibly be used for claims verification purposes. This is achieved by using the GSM chip present on the OBE to send an SMS from the system to the insurance provider indicating the date, time and odometer reading of the vehicle. Once the pre-paid card is topped up, another system SMS is generated, indicating the date, time and odometer reading from when the vehicle is driven insured. To preserve privacy, the GSM chip is silent at all other times. This procedure is analogous to driving the vehicle without renewing an insurance policy, and it is the insured's responsibility to maintain sufficient credit in the smart-card. The payment mechanism used here is offline anonymous digital cash, which is the most complex form of e-cash. There could be scenarios of double spending (Law, Sabett, & Solinas, 1996; Wayner, 1996) where a malicious individual can top up a smart card with digital cash, clone this card and try to use both for paying for insurance premiums. To handle this, the on-board computing device maintains a list of e-cash tokens received in past transactions, so that when the copied smart card is used the system denies insurance and reports this scenario to the insurance provider using an SMS. To prevent using the same card on another vehicle, the OBE is equipped with a writer too, which writes on to the smart card which digital tokens have been used. Upon recharge, the card gets rewritten with new digital tokens.

User Interface

Figure 7.3 is a snapshot of a typical user interface for this privacy-aware insurance model. There are two screens, one containing a dial quite similar to a
speedometer which reflects the final output of the premium payment equation and indicates the cents charged per kilometer in realtime. The digital value is also shown on the same screen. If the anonymous smart-card is plugged in, then the total credit is also visible in the top right corner of this screen. The second screen shows horizontal bars of individual risks such as speed, visibility, weather, road and time respectively, which are adjusted according to conditions. For instance, if the speed is brought within the current speed limit, the speed risk would accordingly slide to the left.

Data Exchange with Insurance Provider

Designing the risk assessment system on-board solves privacy issues associated with transmission of sensitive location information. However, there must be adequate mechanisms to report the system status to the insurance provider. The OBE reports system health to the insurance provider periodically, normally on a daily basis. Public key cryptography is used for ensuring encrypted communication. The OBE device as well as the insurer has a public/private key pair. The insurer’s public key 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 not 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.

Additionally, since there is no transmission of location information, there should be sufficient modelling data made available for actuarial experts to determine new rating variables, as well as to improve the quality of existing rating variables, because automobile insurance is a continuous refinement process (Farid, J., personal communication, 12 April, 2006). Statistical data that give the 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 anonymised and aggregated data with no identification details is performed.

Irrefutable evidence of payments

To prevent cheating and to verify that the OBE is performing correctly, the design provides a mechanism to support non-repudiation. A cryptographic hash function is used to perform this task. The cryptographic hash is a function which takes a long string as input and returns a fixed-sized string as an output known as the hash value (Preneel, 1992) and has the following properties:

- Given the hash value \( h \) it would be hard to find any message \( m \) such that \( h = \text{hash}(m) \)

- Given an input message \( m_1 \), it would be hard to find another message \( m_2 \) (not equal to \( m_1 \)) such that \( \text{hash}(m_1) = \text{hash}(m_2) \)
In order to prove in the future that the total distance was indeed generated as a result of travel on different roads, the system logs the \((x, y, z)\) coordinates received from the GPS receiver along-with the GPS time, in the form of GPS week number \(w\), and seconds elapsed since the start of the week \(s\), which is obtained from the ‘navigation message’ received from the GPS satellite (Borre, Akos, Bertelsen, Rinder, & Jensen, 2007). This combination of \((x, y, z, w, s)\) identifies that the vehicle was on a particular stretch of road on a particular time. For both pre-paid and post-paid systems the cryptographic hash of the sum of all \((x, y, z, w, s)\) tuples is generated once every billing cycle (monthly) and is essentially the hash of tuples described above, consolidated on a monthly basis. As shown in Figure 7.4 a hash function is computed on this message. GPS data for the last running month is simultaneously stored and encrypted with the dispute resolution office’s public key. For confidentiality, the total premium and total distance travelled in the last billing cycle is then encrypted with the insurer’s public key and concatenated with the hash value \(H\) and sent to the insurer via the GSM network. The insurer strips off the hash value and stores it and decrypts the remaining message using its private key to obtain the transmitted distance and premium values. If the setup is post-paid, the insurer generates an invoice and sends it the insured party for payment receipt. For pre-pay systems, it logs this data in its records.

To address any disputes the log history of the last running month is retained on the OBE as mentioned earlier. It is encrypted with the public key of an Insurance Ombudsman Service (IOS) or dispute-resolutions office, which would be a trusted third-party (Insurance Ombudsman Australia, 2008). If the insurance provider has concerns about the premium charged in a particular month (an extremely low or extremely high value), it can approach the IOS office with the hash function it received for that particular month. The dispute-resolutions office would then ask the motorist to disclose the entire GPS log to it (which is
202 7. User-Perception Inspired Privacy-Aware Models

*Processing on OBU*

- **P**
- **||**
- **D**
- **Enc**
- **Enc(Σ(x,y,z,w,s))**
- **||**
- **P_{k_{ins}}**
- **Enc(Σ(x,y,z,w,s))**
- **H(\Sigma(x,y,z,w,s))**
- **Enc**
- **Enc(I(x,y,z,w,s))**
- **Dec**
- **I'(x,y,z,w,s)**
- **GSM Network**
- **H**
- **Dec**
- **P**
- **D**

*Processing at Insurer’s side*

Where,

- **P** = Total Premium in Dollars
- **D** = Total Distance in Kms.
- **Σ(x,y,z,w,s)** = GPS positions + GPS Time
- **H** = Hash Value
- **Enc** = Encryption
- **Dec** = Decryption Function
- **||** = Concatenation
- **P_{k_{ins}}** = Public key (insurer)
- **P_{k_{dis}}** = Private key (insurer)
- **P_{k_{dis}}** = Public key (dispute resolution)
- **P_{v_{dis}}** = Private key (dispute resolution)

\[ H(σ) = H(δ) \]  

*Figure 7.4: Dispute Resolution Protocol.*

stored on the insured’s OBE) as shown in Figure 7.4. The dispute-resolution office would then decrypt this data using its privacy key and apply the hash function and verify that the output is the same hash value that was provided by the motorist to the insurance provider, and purge the contents from its memory. In this way, dispute resolution is performed with the help of a trusted third party, and at no point does the insurance provider get access to precise positional data of the insured.
7. User-Perception Inspired Privacy-Aware Models

7.2.6 System Evaluation

Security of Device

The privacy-aware GPS-enabled insurance design presented here depends on the correct functioning of various sensors, such as the GPS receiver, humidity and light sensors. Since this is a payment system, it is essential that tamper resistance be built in to the system, as a technically savvy motorist would be motivated to cheat the system in order to gain additional savings. As mentioned earlier, the device sends an SMS everyday to the insurance provider reporting system health. Power to the OBE and these sensors should be linked to the ignition switch, such that tampering with power or power disruptions to these sensors or the OBE transmits a system-tamper or malfunction SMS to the insurer.

Another area of potential concern is tampering of positioning signals received by the GPS receiver. Chapter 5 discussed the possibility of sending fake GPS signals to a target GPS receiver with specialized signal simulator hardware. Various software-based countermeasures were also discussed there, ranging from Doppler shift checks to monitoring relative signal strengths, which can be implemented within the GPS receiver (Wen, Huang, Dyer, Archinal, & Fagau, 2005). If such an attack is detected, the GPS receiver can inform the OBE of potential spoofing, which in turn can be relayed to the insurance provider for investigation.

To ensure the confidentiality of data, communication between the insurer and the insured is encrypted using the public key of the insurance provider. The insured party appends their contract identifier to all communications to identify that the message originated from them. GPS data stored on the OBE is not stored in clear-text, as mentioned earlier: it is stored as cypher-text encrypted with the dispute-resolution office’s public key. Once logged, even the customer does not have access to the previous month’s movements, and this information is stored there for the sole purpose of resolving disputes.
Cost

The privacy-aware design proposed in this thesis depends on existing telematics platforms that are available in high-end luxury cars and are slowly permeating into the mid-range and smaller models. Satellite navigation already provides spatial maps of the road, alerting the motorist of enforceable school zone speed limits (currently 40 KM/hr), speed cameras and red light cameras (Road Angel, 2004). As discussed in Chapter 2, RSW are being offered on mid-range to small cars, sometimes as a standard feature (BMW Australia, 2008; Hyundai Azera, 2008; RainTracker, 2008). Sensors to activate headlight lamps and rear and front parking sensors are also becoming increasingly available.

All these tools can be used to design a system that is capable of measuring real-time risk on-board, with minimal infrastructure costs. The only additional cost may be in using a GSM chip for transmission, making available a spatial database of road-risks and speeds, and on-going costs in maintaining the system. The cost of SMS transmission has also been kept to a minimum here since there is one SMS per day notifying the health of the system, and an additional SMS per month for transmission of computed premiums and distances; far less than the GPS/GSM insurance systems already on the market.

Potential Benefits

Savings

As compared to the current implementations of GPS-enabled insurance, this architecture minimises the transmission of data from the insured to the insurer. Apart from the privacy benefits, there are also savings in the long term as there is a cost involved in using SMS or other mobile communication methods which would eventually be reflected in the premium that an insured pays. Additionally, the heavy reliance on the GSM network would cause system failure in areas where there are GSM outages, as mentioned earlier in Chapter 4.
Accurate and fair reflection of risks
Proponents of distance-based charging have been saying that a fairer reflection of insurance risks would make insurance affordable and motivate motorists to be more economical, as the fixed cost of insurance would become variable depending on how much the vehicle is driven. The privacy-aware design proposed in this chapter surpasses these benefits by being an accurate reflection of risks. As compared to distance-based charging, this design is capable of taking other risks such as speed and road conditions into account. Variable insurance premiums based on actual risks would encourage the insured to be safe drivers.

Risk-enabled route navigation
RDS-TMC is an international standard for delivery of traffic information to on-board satellite navigation systems, using broadcast radio channels such as FM or AM (Intelematics, 2008; myDrive, 2008). Using these transmissions navigation systems can allow drivers to dynamically use alternative routes thus avoiding congested thoroughfares. A similar idea can be implemented in the proposed privacy-aware insurance design to route from source to destination avoiding high-risk roads and minimising insurance costs, since there is a spatial database within the vehicle which risks associated with different roads. This feature would be quite similar to the available trip-planners which let the motorist route alternate paths based on shortest distance or avoiding tolls, etc.

Privacy as a Business Strategy
As sensitivities about access to and retention of personal data increase, organisations have started to appreciate that privacy can be used as a business strategy, A company in France has secured two French design patents for privacy-friendly pay-as-you drive insurance where, similar to the design proposed in this Chapter,
they propose to aggregate GPS data on-board and send statistical data to the insurance provider. They have made licences available for interested insurance companies seeking to adopt this technology in their PAYD solutions (Troncoso, Danezis, Kosta, & Preneel, 2007; Ebonis, 2008).

Real Insurance (2008) is the first Australian insurance company to have proposed a distance-based model which solves most of the privacy issues by taking the simplest approach. They use MRF, as discussed in Chapter 4; however they do not require independent verification of the kilometres used in a premium cycle and rely on the honesty of the insured to provide them with actual odometer readings.

Progressive Insurance in the US, which patented the technology of using the combination of GPS and mobile phones to transmit movement data to an insurance server, is actually pursuing a different differentiated pricing paradigm which involves no location tracking. It is known as TripSense and uses the OBD-II port for collecting data. This system has been rolled out nationwide and is being marketed as MyRate (2008). In this approach motorists are offered a device that connects to the OBD-II port and collects data based on how, when and how much the vehicle is driven (not ‘where’). Drivers upload this data voluntarily to receive discounts. They might end up paying more if there is indication of excessive risks being taken, but since this is a voluntary system the individual decides if he/she wants to disclose this data.

Norwich Union’s rollback of the PAYD program (Howard, 2008), and the cautious approach taken by other insurers indicate that they are aware of the public concern associated with release of precise movements and want to avoid these scenarios. The privacy-aware GPS-enabled insurance design as presented in this thesis offers spatial privacy protection without compromising the associated benefits of accurate risk estimation.
7.2.7 Conclusion

It has been shown here that only a federated system has the capability of retaining true anonymity for motorists' movement data. Additionally, a federated system has a higher possibility of analysing sensory inputs and quantifying risks from them to be used for premium processing, yielding a fairer reflection of actuarial accuracy. Cars have become mobile computing platforms and should be used as intelligent sensors to process data, rather than having all data transmitted back to base for processing, which not only creates a communication bottleneck, but also enables mass-surveillance. By implementing the payment system on-board, insurers have the capability of taking real-time risks into account and gaining actuarial accuracy. In advocating the consumer’s privacy interests, a reasonable balance has been maintained by proposing a privacy-respecting insurance model, with necessary analysis data provided to insurers.
7.3 Post-Paid Anonymous Toll Collection

Sections 7.3.1-7.3.3 summarise the recommendations that were made in Chapters 4, 5 and 6 for a privacy-aware toll collection model. Sections 7.3.4-7.3.7 present an anonymous toll solution using these critical recommendations in the proposed design.

7.3.1 Results on ETC from the Privacy Analytical Framework

ETC was categorised as an active system in the analysis presented in Chapter 4, since the toll gantries are clearly visible and the motorist is aware that taking a particular route involving tolls will register their vehicle details in an ETC database, including the time and location the passage took place. Should the motorist wish to avoid this happening, they may take an alternative route not involving tolls. However, this strategy will not be effective when all routes leading to a particular destination have toll gantries installed.

The spatial-resolution of tolls depends on the density of toll gantries in a particular region and the routes that an individual takes. It has also been noted that the choice that motorists have in adopting GPS-enabled insurance is not available in the case of tolls, and motorists are in this case required to surrender their privacy, since tolling systems are gradually being converted to being exclusively cashless. It has also been discussed that the analogy for ETC systems in the non-electronic world means that a toll booth operator collects the toll amount, photographs the vehicle’s number plate, notes down the time, date and location where the toll event occurred, and stores this recorded data for up to a period of seven years. Although it would be completely feasible to expunge trip details once the toll fees are received, it appears that this data is held indefinitely, in the hope that it might have a future use. These important issues help alert
to the fact that the transformation of tolls from the non-electronic world to the electronic world threatens the freedom of movement that motorists have enjoyed up till now. The proposed design aims to achieve a complete incorporation of these ignored aspects into a privacy-aware tolling model.

### 7.3.2 Survey Results on ETC

Toll-related survey results presented in Chapter 6 are revisited in this section in order to channel significant recommendations as input to the proposed privacy-aware toll collection design.

The survey results suggest that motorists considered tolls more invasive as compared to mobile phones. Intuitively, mobile-phone-based positioning would have a higher resolution, but respondents thought that they had a choice of switching off the mobile phone, while toll tags would be required to travel on the growing network of cashless toll routes.

The survey results also indicate that for nearly 66% of respondents the median interest in anonymous tolling, (on a scale of 1-10) was 7, which is a strong indicator that the current community is aware of the threats to privacy with tracking and the retrospective capabilities of toll data. The last survey related to tolls and privacy in an Australian context was carried out almost a decade ago, when 28% expressed concern about their movements being stored electronically, and 73% cited invasion of privacy as the reason for their concern (Ogden, 2001). It appears that community perceptions with regards to privacy and freedom of movement have evolved since this time probably because the majority of the respondents (60%) were aware that cashless tolling would be implemented in NSW in the next few years.

It has been discussed in Chapter 4 that the privacy-protecting features that were promised/existed when ETC was rolled out have vanished with the passage of time. The aim of the survey was to understand what issues prompted
the decline in anonymous options. Is there a relation between convenience and privacy? Do motorists want privacy-features without being financially disadvantaged? For instance, it is possible that with an anonymous pre-paid system, a motorist who wants to remain anonymous is not willing to sign up and invest $50 in topping up a card when they only occasionally use toll roads. In summary, privacy-respecting features that were made available in past applications often did not attract significant attention, leading to a gradual phasing-out of those options because of the administrative burdens imposed on those who might have otherwise wished to use them.

For this reason, respondents were asked if they preferred pre-payment or post-payment for the anonymous tolling system. The majority of the respondents (63%) preferred an anonymous post-paid solution. Survey results suggest that, from a motorist’s perspective, the payment method also plays a critical role when feasibility in pursuing privacy is assessed. In short, a successful business model for privacy-aware tolling has to be capable of providing both post-paid and pre-paid payment methods.

7.3.3 Protocol Requirements

1. An honest motorist is able to pay toll charges anonymously.

2. The protocol offers post-paid payment features.

3. Toll providers should not be able to reconstruct the trips of patrons.

4. Toll operators receive correct toll charges for all vehicles passing their gantries without the need to identify them.

5. Anonymity guarantees are for customers only. Motorists without a valid E-Tag or ones who have tampered with their transponders forfeit their right to anonymity.
6. Only vehicles that fall under condition 5 would be photographed for enforcement purposes.

7.3.4 Cryptographic Building Blocks

The protocol presented here uses techniques from cryptography to preserve the anonymity of the motorist, and guarantees that the toll operator would receive the total charges for all trips made by all registered motorists. This protocol prevents anonymous payees from being disadvantaged, by offering a post-pay anonymous system.

Various electronic payment systems have been proposed by researchers that offer anonymity for performing business transactions (Heikkilä & Laukka, 1999; Camenisch, Piveteau, & Stadler, 1996). Most of them exploit cryptographic primitives of digital signatures, blind digital signatures and zero knowledge proofs (Chaum, 1983; Goldreich, 2001; Rivest, Shamir, & Adelman, 1978). The protocol presented here uses blind digital signatures and zero-knowledge proofs for anonymous toll collection.

**Blind Digital Signatures**

In cryptography a blind signature, as introduced by Chaum (1983), is a form of digital signature in which the content of a message is blinded before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. The only difference is that the signing party does not know the contents so is not able associate an identity with an unblinded message. Blind signatures with their inherent privacy-protecting features are suitable for anonymous tolling.
Zero-knowledge Proof

Zero-knowledge proof is an interactive method for one party to prove to another that a statement is true, without revealing anything other than the veracity of the statement (Goldreich, 2001). A zero-knowledge proof must satisfy three properties:

**Completeness:** If the statement is true, the honest verifier will be convinced of this fact by an honest prover.

**Soundness:** If the statement is false, no cheating prover can convince the honest verifier that it is true.

**Zero-knowledge:** If the statement is true, no cheating verifier learns anything other than this fact.

Commitment Scheme

This scheme consists of two operations, LOCK and OPEN (Goldreich, 2001). The sender can lock a message using LOCK and send it to the receiver in the commit phase. In the reveal phase of the protocol the receiver gets the key to open the lock to see what is inside. Thus, \( \text{LOCK}(x) \rightarrow (a,b) \) takes as input a message \( x \) and produces the pair \( (a,b) \), where ‘a’ is the ‘safe’ and ‘b’ is the ‘secret opening value’. The recipient is sent \( a \) first. At a later stage when it is sent \( b \), it can apply \( \text{OPEN}(a,b) \rightarrow x \) to obtain the original message.

7.3.5 Conceptual Design

The use of multiple identifiers rather than one unique identifier in the context of RFID privacy has been proposed earlier (Juels, 2005). Blumberg, Keeler, et Shelat (2005) proposed a similar solution to the use of multiple identifiers in their design of a camera-less traffic enforcement system. To preserve motorists’
### Proposed Toll Protocol

<table>
<thead>
<tr>
<th>Registration</th>
<th>Toll Event</th>
<th>Debt Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Registration</td>
<td>Customer produces authorised identity</td>
<td>Hashes Accounts Receivable</td>
</tr>
<tr>
<td>Customer generates multiple identities</td>
<td>Token logged in accounts receivable database</td>
<td>Zero Knowledge Proof</td>
</tr>
<tr>
<td>Customer signs each identity with own digital signature</td>
<td>Gantry verifies toll authority signature</td>
<td>Invoice generation and settlement</td>
</tr>
<tr>
<td>For Each identity</td>
<td>Unauthorise</td>
<td>Dispute</td>
</tr>
<tr>
<td>H = Hash function generated for series of identities</td>
<td>Photograph Licence Plate</td>
<td>No</td>
</tr>
<tr>
<td>H is stored in Database</td>
<td>Proceed Infringement Processing</td>
<td>Dispute Resolution</td>
</tr>
<tr>
<td>Toll Authority Receives H + Encrypted and Signed Identities</td>
<td>A Blind Digital</td>
<td></td>
</tr>
<tr>
<td>For Each Encrypted Identifier</td>
<td>Signature For Each Identity</td>
<td></td>
</tr>
<tr>
<td>Passes Certificates to Customer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer has authorised digital identities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 7.5: Steps involved in registration, toll event and toll collection.
privacy in the case of traffic infractions the protocol reveals a different identity each time, which the infringement processing centre stores for collection. When registration of the vehicle is due for renewal the motorist and road authority compute the fines that a motorist has to pay, based on those identifiers.

The solution presented here for post-paid anonymous tolls is largely based on Blumberg et al.'s initial work and extends it to be customised to the tolling industry. Tolls can be either 'closed-systems', where toll is calculated based on the distance travelled, or 'open-systems', where toll is charged for passing a particular toll gantry; therefore the protocol is modeled to cover both these scenarios.

Instead of a unique E-tag identifier, multiple digital identities for the E-Tag are used. The vehicle discloses a different identifier to a toll gantry at every toll instance, so neither a toll gantry nor toll providers' payment processing systems can erect the motorist's travel profiles. The protocol consists of three stages: registration, toll event, and payment as illustrated in Figure 7.5 and discussed below.

**Registration:** The motorist approaches the toll provider and signs a contract to use the toll roads. The motorist receives an RFID transponder and bootstraps it with a set of digital identities randomly drawn from a sufficiently large pool. These digital identities are used when the motorist is required to disclose their identity when approaching a toll gantry. The motorist provides a one-way cryptographic hash of the set of digital identities to the toll provider so that they can not disavow their identities later at the time of toll collection. Each of these digital identities are blinded by the motorist and then given to the toll provider to perform a blind signature for each of them. This blind signature can be verified at the time of a toll event.
Figure 7.6: Spatio-temporal details of trip stored in motorist's transponder.

**Toll Event:** At every toll event the toll gantry sends its digital certificate to the motorist and the type of tolling system it is (O for open-system, C for closed-system) for authentication as an authority to collect toll. After authentication, the motorist's transponder discloses a digital identifier, and its associated blind signature selected randomly from its pool of identifiers. This randomness prevents the toll provider from erecting travel profiles of the motorists. The used identifiers are stored in a 'used list' by the motorist's transponder. The toll gantry verifies that the blinded message is indeed generated by the toll provider for the digital identity disclosed.

If the tolling system has distance-based tolling implemented, then the revealed identifier is used as a session-identity (or temporary alias) and is cached in the gantry's memory, which looks for the same identifier at the exit points of the tolled road. The motorist's transponder is required to send the same identifier it sent earlier upon entry to the tolled road, which is then used by the RSE to...
determine the price of the tolled distance. It then sends the digital identity and the toll fee to the toll provider’s computing server for future revenue collection. The spatio-temporal attributes, such as the time of the toll event and place are not stored on the server. To avoid erection of travel profiles in the future, this information is instead annotated to the list of used identifiers in the motorists’ transponder as illustrated in Figure 7.6.

If the motorist does not provide a valid digital identity set, they lose the right to travel anonymously, and the toll gantry system, activates the enforcement system which takes a picture of the vehicle’s licence plate for fine enforcement.

**Bill Generation and Id Renewal:** At the end of the billing cycle the motorist discloses in zero knowledge their list of used identifiers to the toll provider. The toll provider makes its revenue collection list public, and an intersection of the motorist’s used list and the toll provider’s revenue collection list is computed in zero-knowledge for bill generation. At payment processing the motorist again generates digital identities for the next cycle.
7.3.6 Protocol Details

The protocol requires 4 entities (Figure 7.7(a)), namely the toll collection company ‘E’, the motorist transponder ‘M’, the toll gantry ‘G’, and a video enforcement system ‘V’. There are 3 steps involved in the protocol (Figure 7.7(b)), namely registration, toll event and toll collection, which operate sequentially.

E and M have a pair of public/private keys, which are pk_E/pv_E and pk_M/pv_M, respectively. The motorist’s transponder also contains a cryptographic hash function H_M, which is used to compute a one-way hash of the list of identifiers. The toll gantry G has a digital certificate which has been issued by the toll provider E to act on its behalf and collect the identifiers when vehicles pass the gantry. This is done to prevent cloning of M’s identifiers by adversaries who could simply listen in and use the intercepted identities for impersonation.

1. Registration

(a) This stage uses the public/private key pairs pk_E/pv_E, pk_M/pv_M and the hash function H_M.

(b) M randomly generates a list of identities drawn from a sufficiently large pool.

D = \{id_{i_1}, id_{i_2}, id_{i_3}, id_{i_4}, id_{i_5}, id_{i_6}, ... id_{i_{mk}}\}. It is expected that these identities or tickets would be large enough in number, so that one ticket is disclosed per gantry entry.

(c) M computes a commitment by computing LOCK(id_{ij}) \rightarrow (a_{ij}, b_{ij}) and sends a sequence of commitments (a_{i_1}, a_{i_2}, a_{i_3}, ... a_{i_{mk}}) to E along with a hash value h which is obtained by applying the function H_M to the list of generated tickets.

(d) For each index i in the list D, M randomly assigns c_i = a or c_i = b and then sends to E a list of \(c_1, c_2, ..., c_n\).
(c) $M$ reveals the commitments for each challenge $c_i$, by sending $b_{ni}$, to prove that it knows each of the tokens it has generated. The remaining unopened sequences are renamed as $(id_1, id_2, \ldots, id_n)$ and the remaining corresponding commitments as $(a_1, a_2, \ldots, a_n)$.

(f) $M$ and $E$ engage in a blind signature protocol where $E$ generates a blind signature for each pair $(i, id_i)$. Let these be denoted by $\sigma_i$ for each $(i, id_i)$.

2. Toll event

(a) When $G$ senses a vehicle is in communication range it sends an authentication message consisting of a digital certificate signed by $E$ and the type of tolling system (O: Open or C: Closed) it is.

(b) Once $M$ is satisfied that $G$ is an authentic toll event logger, $M$ sends it $(id_t, \sigma_t)$ and its class of vehicle (C: car, T: truck, M: motorcycle, B: bus).

(c) $G$ applies a blind digital verification protocol and verifies that the signature $\sigma_t$ originated from $E$, and that the $id_t$ provided is valid.

(d) For settling payments.

   i. **Open System**: $G$ determines the toll charges, \('ch'\) on the class of vehicle, and sends the tuple consisting of $(ch, id_t)$ across to $E$, where $E$ stores it in a list of toll receivables.

   ii. **Closed System**: Where distance-based tolling is implemented, the ticket $id_t$ disclosed by $M$ is buffered in cache memory at the $G$. $M$ notes that it was a closed system in initial handshake and is required to disclose the same ticket value when taking an exit on the tolled road. The exit points have transmitters installed which broadcast a signal indicating that the exit is approaching, along with the toll charges for each class for that particular exit. $G$ looks
Motorist
(GantryId, CertTollType)
(id, DigSig, VehicleType)
(id)
ANPR_LicencePlate

Gantry

Visual Enforcement

If id not in list
Alert

Figure 7.8: Sequence of message exchange in a closed tolling system.

for ticket values that have already been transmitted to it upon entry and expects a token from M that matches its entries. M releases the same \( id_t \), which is used by G to calculate toll charges based on the distance-tolling protocol for that particular class of vehicle. The value ‘\( ch \)’ is then included in the tuple consisting of \((ch, id_t)\) and sent across to E, where E stores it in a list of toll receivables.

(e) G only transmits the charges and the digital ticket identity to E. Only M stores the spatio-temporal attributes in its records for information, otherwise it would be possible to retrospectively erect a driver’s travel profile if the time and place can be related to the ticket and the motorist.

(f) If M does not provide an identifier or provides a forged identifier which does not pass the verification test, G activates V to photograph the licence plate as evidence for infringement processing, as illustrated in
3. Bill collection and digital identity renewal

(a) At the end of the billing cycle, $M$ and $E$ engage in a reconciliation protocol, where $M$ computes the intersection of its used identities list \((uid_1, uid_2, ..., uid_k)\) and $E$'s toll receivables list \((rid_1, rid_2, ..., rid_m)\).

(b) $M$ opens the commitments for this intersecting list \((b_1, b_2, ..., b_k)\) to prove to $E$ that it indeed incurred these charges.

(c) $M$ then proves in zero-knowledge that all its identities in the tolls receivables list have been accounted for.

(d) $E$ can also ask $M$ to disclose the whole list of the initial identities and function $H_M$, and can reapply the hash to check if the hash value computed matches the one provided at the start of the protocol in order to detect cheating.

(e) If $E$ is satisfied, it generates a bill for the charges, and the registration process is repeated.

7.3.7 Other Implementation Options

Sections 7.3.3-7.3.6 discussed the anonymous post-paid solution. This section reviews prepaid solutions for anonymity and also draws the reader’s attention to an infrastructure-less tolling architecture which can be achieved by utilising the framework setup described in Section 7.2.

Pre-Paid Anonymity

Many toll providers allow motorists to pay tolls with prepaid accounts. One would assume that prepaid accounts would be quite similar to prepaid mobile accounts, by which anybody can buy a Subscriber Identity Module (SIM) start-up kit from a convenience store and be ready to make mobile phone calls. This
7. User-Perception Inspired Privacy-Aware Models

has not been the case in prepaid toll operations. A fairly recent launch of toll operations to reduce congestion on roads in Dubai, United Arab Emirates, using sophisticated passive RFID tags (no batteries required) also has similar privacy-related issues (Salik, 2008). This system could work perfectly without identifying the vehicle, but they still require motorists to register their vehicle details, personal details and a mobile phone number on the pretext of using this information to send an SMS when the credit falls below a certain threshold value, and stores all transaction details including trip histories. One can argue that instead of sending an SMS, the tag can indicate that it has gone below a certain limit by emitting a distinct beep sound.

The only reason to store a transaction should be to claim payments from a customer. Once that is settled there should be no other reason to still maintain these details in permanent storage. Prepaid systems can inherently respect the privacy of motorists if they are designed with a ‘privacy-friendly attitude’. Prepaid toll kits should be made available that can be bought by anybody for a particular class of vehicle, and used without the need for registering identification/licence details anywhere. As the vehicle shoots through the tolls, the reader/writer deducts the appropriate fee from the toll tag, eliminating the need for storing any personal information.

7.3.8 Conclusion

It has been demonstrated above that the simple cryptographic technique described can be utilised to preserve the anonymity of a motorist, and does not disadvantage them by requiring pre-payment for their tolls. Privacy is preserved due to the fact that the toll provider does not know anything more than the hash value of the list of identities. The motorist cannot cheat because it has provided the hash function in advance, and proves in zero-knowledge all the trips it made. The motorists’ trips cannot be reconstructed by the toll provider at any stage.
7.4 Infrastructureless Tolls and Insurance

One of the advantages of GPS-based systems is their ability to adapt easily and quickly to changes in charge parameters (road classes, vehicle types, emission levels, time slots, etc.). This concept of postpaid anonymity can also be taken one step further by exploiting developments in the field of telematics and reduce costs associated with maintaining road-side toll infrastructure.

The privacy-aware insurance model presented in Section 7.2 is a framework with a spatial map of the road network, which is used in coordination with a GPS receiver to compute trip aggregates. The same map can also be bootstrapped with the location of roads where toll fee is applicable and the role of the toll gantry \( G \) discussed in the previous anonymous system can be modeled on the on-board computer. The OBE can be bootstrapped with the locations of all the toll road stretches. When the vehicle’s GPS position is within the bounds of the toll locations, a logging event can be activated that can collect the vehicle’s current digital identity, and the blind signature previously discussed and store it in a secure storage area. The motorist does not have access to this secure storage area within the OBE, and cannot tamper with it.

At the billing cycle, the motorist engages in the same protocol whereby the toll provider receives the toll payments for the list of used identities and locations present on the secure storage in the vehicle. Only the toll provider can read from this area, and only the event logger can write to it.

The motivation here is to have an integrated device that performs various functions and preserves the anonymity of motorists. Additionally, once these devices are pervasive, there would not be a need to maintain an ETC infrastructure and installation and maintenance of expensive RSE. The intelligent vehicle would compute where it has been, and make payments for tolls, insurance and parking. The use of a common hardware for these various services ensures that the start-up costs for users and service providers can be minimized. The com-
combination of tolls and insurance on one platform that preserve motorists' privacy can improve overall user acceptance of both these systems.

7.5 Summary

In the past, motorists have enjoyed some form of anonymity on roads. Unfortunately the trend of providing customised and contextualised services such as assisted parking, electronic tolls and mobility-priced insurance have not catered to the much desired anonymity principle when these systems are transferred from the non-electronic world to the electronic world. In existing electronic pricing systems cars need to be identified to be correctly priced for taxation, levies, insurance, toll or a service.

In this chapter a critical analysis of the privacy issues, a comprehensive assessment of threats and vulnerabilities of position data, and community perception towards privacy and pricing have been used as a direct input into the design of two privacy-aware road pricing systems. It is clear that the community is an important stake-holder and seeking the public's opinion proactively and designing solutions around their perspectives means that these systems are likely to be adopted when they are presented.

Additionally, the traditional client/server model where data is pushed to a server for payment processing makes spatial data susceptible to abuse. Even anonymity does not seem to be able to prevent this, given the power of inferencing with high resolution GPS data. With the knowledge of a vehicle's location, a reasonable guess can be made about the activity involved. If such movements are studied over a long period of time, then there is a high probability of making accurate inferences. Since mobility-pricing would be a perpetual process, such travel profiles would be quite representative of an individual's life.

Vehicles are evolving into sentient computing environments and new vehicle-centric processing approaches can be visualised in the future. Satellite Navigation
(SATNAV) is slowly permeating into the small to medium range vehicle models and this framework could be utilised to perform computations in-vehicle rather than sending information back to a central computing authority.
Chapter 8

Conclusion

8.1 Summary of Results

The aim of this thesis has been to design privacy-aware models for mobility-pricing, taking into account the user's perspective and other societal factors. A critical technical analysis of issues has shown that a recalibration of information practices is required. The most important issue in preserving privacy on roads is the restoration of anonymous travel. Although it is often treated superficially in the literature on privacy, anonymity is a necessary component of privacy. The control of one's own identity depends on the ability to remain anonymous. Since precise location information has the potential to reveal the identity of motorists, the disclosure of location information has to be aggregated or not disclosed at all in order to preserve privacy. The ability to conduct one's affairs on roads anonymously, while having the ability to pay tolls and to draw benefits from a fair pricing system without having to systematically identify oneself is the problem that this thesis has tried to address.

In order to examine the key challenges involved in this recalibration, an analytical framework was developed in Chapter 4 which evaluated the key issues, initially by reverse engineering current electronic systems to a manual process
and establishing the amounts of data gathered about a motorist. This framework also identified the type of surveillance enabled by these systems, the precision of information collected, and their capacity to be embedded in a motorist’s life. The analysis also yielded a number of policy recommendations, which highlighted the need to consider anonymity as an essential aspect in the design of a privacy-aware system.

Chapter 5 supplemented these findings by analysing the threats to personal autonomy and personal privacy represented by the collection of precise GPS data. This chapter demonstrated the threat of the ability to infer behaviour and personalities from even de-identified GPS data. An inferential engine was developed which could identify the class of people one belonged to (in this case: student, academic or support staff), on the basis of their GPS movements, and which also allowed the probable home locations and road behaviours of subjects to be inferred. This exercise established that precise de-identified location information can still be related back to identifiable individuals by the use of such inferencing, and by utilising existing geo-informational databases. It is therefore recommended that to preserve motorists’ privacy in the context of GPS-based transactions alternative designs that do not disclose precise GPS information should be explored. A federated approach is recommended that prevents disclosure of precise movements, thus discouraging centralised settings. Another issue of significance examined here was that of the technical vulnerabilities of these systems, which could be exploited by motivated individuals intent on cheating the system to evade financial or criminal penalties. It is thus recommended that GPS-based pricing approaches should take these vulnerabilities into account, especially if a federated approach is to be employed, where the provider implicitly trusts the federated system to collect accurate charges on its behalf, and that systems are designed that are tamper-proof as well as being capable of withstanding intentional attacks.
8. Conclusion

Having looked in detail at the technical aspects, the next step employed in this research was to investigate the social contexts of the problem. It has been noted in the literature that previous attempts at providing anonymity have declined over the passage of time. This situation has demonstrated the possible relationship between perceived privacy and economic or physical inconvenience. Motorists are likely to wish to have their movement information preserved/retained if it is seen as a necessary part of the process of registering in and using the system. The majority are unlikely to go out of their way to achieve true anonymity. The survey results in Chapter 6 also suggest that motorists do not want to be disadvantaged in choosing a particular type of payment option if they have a greater appreciation for privacy. The survey results indicate that in the context of electronic tolls post-paid anonymity is regarded as a desirable quality. The results of the survey also demonstrated that respondents considered privacy-respecting technologies as an essential tool: one that is more important than specific legislation to preserve privacy on roads. A qualitative analysis of survey responses highlighted other important issues, such as the legal implications for disclosure of precise location information if it is used to penalise motorists.

Finally, in Chapter 7, all the recommendations and key results discussed in Chapters 4 - 6 are combined into a coherent whole and are used to construct privacy-aware technological designs which bridge the entire array of privacy interests and combine them into a unified approach that is able to satisfy the privacy requirements of motorists as well as to offer assurances of accurate payment collection to service providers. For electronic tolls, a post-paid anonymous solution is presented. In the case of GPS-enabled insurance, a federated pay-how-you-drive system is proposed. It has been shown that federated systems have a higher possibility of analysing sensory inputs and quantifying risks. The argument presented here is that cars are mobile computing platforms and are
able to perform such calculations, rather than acting as conduits to channel all the data to a centralised system. In advocating the consumer’s privacy interest, it is believed that a reasonable balance has been maintained by proposing privacy-respecting alternatives that do not disadvantage either motorists or service providers.

Tolerating corporate or governmental privacy intrusions is a slippery slope, since allowing such treatment reduces expectations of privacy and softens up the community for future intrusions. There is a serious need for the recalibration of policy and for greater sensitivity towards privacy issues, especially as cashless operation is expected to be the only mode of road-pricing in the future. A basic tenet of good privacy policy is that information that is not needed should not be collected in the first place and certainly should not be stored for long periods. The mere existence of the data invites retrospective abuse. This phenomenon is repeatedly observed across the entire spectrum of privacy issues. At present, little or no thought has generally been given as to how the data now commonly collected, which can contain location sensitive information, could be abused. It has been demonstrated in this thesis that anonymous solutions are quite plausible. It is hoped that the designs presented in this thesis could provide a basis for the design of future toll and other road transport applications and thus prevent further erosion of privacy in this arena.

8.2 Thesis Limitations

There are some practical, methodological, and theoretical limitations which need to be taken into account when analysing the results of this study. Firstly, when analysing the user perspective towards privacy-aware mobility-pricing systems, this thesis has been more focused on quantitative research methods than qualitative ones. The strength of qualitative research involves collecting information from various sources, even if the analysis of open-ended questions conferred im-
8. Conclusion

Important data for answering the research questions in this study.

Secondly, the algorithms with regards to GPS-enabled insurance focus on re-designing the same insurance product with a privacy perspective. It is acknowledged that developing proper actuarial models for real-time estimation of risks is better addressed in the actuarial sciences.

Finally, the financial costs in recalibrating a server-processing model to an in-vehicle approach has not been within the scope of this thesis. Although the thesis has suggested that processing the data on-board will minimise the costs of data transmission and data archiving, the actual costs have to be accurately gauged by financial planners and decision-makers.

8.3 Future Work

This thesis has focused on designing privacy-aware systems and proposed alternate approaches to road pricing. Future work could be conducted in association with actuarial researchers and transport researchers to further improve these models.

Many other challenges remain with regards to location privacy, both social and political. Questions regarding who should have the right to make privacy decisions about data related to an individual, as well as who owns location information are still open research questions.

This study has attempted to draw together the expertise of both technical and legal experts, but there is clearly considerable scope for significant future collaboration between professionals in both these areas. At the same time social scientists should be involved in further studying privacy attitudes among the public, especially in the Australian context, in order to give clearer insights into what would be acceptable privacy-aware designs for the collection of location information in future.

Actual development of effective privacy laws, and those that address location
information specifically, will be a gradual process. However, with the rapid evolution of technologies, the Law has to begin to revisit these issues rather urgently. Professor Bennet succinctly explains the current situation with regards to location based services

"As with every other surveillance practice, however, it is quite obvious that with respect to location based services as well, activists, analysts and regulators are having to play catchup trying once again to change the tire on a moving car." (Bennett & Crowe, 2005)
Appendix A

Survey Questionnaire:
Preliminary Online Survey

> Watch the movie clip again

User Perspective of Privacy in Telematics - A Survey

Thank you for visiting this survey and watching the movie clip. We hope you now have some idea of the potential threats to privacy with location technologies. Your response in taking this survey is highly appreciated and would help us in designing privacy enhancing telematics technologies. You can now proceed with the survey by optionally providing us with your email address and clicking the "Start Survey" button.

There are 14 questions in the survey and would approximately take 10 minutes

Notice of consent

I hereby consent to participate as a subject in a research project entitled "User perspectives of Privacy in Telematics", conducted by Usman Iqbal and Samsung Lim of the School of Surveying and Spatial Information Systems, University of New South Wales, Australia. I can contact the investigators at +61293854206 or by email at m.iqbal@student.unsw.edu.au NOTE: participation is open to anyone, regardless of computer expertise, age, etc. I understand that I will complete a questionnaire having to do with the use of GPS based telematics and their relation to location privacy. I understand that my participation is completely voluntary, and that I am free to withdraw from the study at any time I choose, without penalty. I understand that this project is not

Please provide us with your email address.
It would be only used to
1) Restore your session, if you wish to leave the survey and come back to it at a later stage.
2) Or, if you would like to receive a research report of the survey results upon completion.
Rest assured that the email address would remain confidential.

Email Address

Start Survey

231
1) Your gender?
- Female
- Male

2) Your age bracket?
- 18-25
- 26-32
- 33-40
- 41-50
- 51-60
- 60+

3) Your area of expertise?
- Positioning technologies
- Information technology
- Sciences
- Arts
- Law
- Engineering
- Health care
- Business
- Accounting
- Other

4) Your driving licence type?
- Learner's Licence
- Provisional Licence (P1)
- Provisional Licence (P2)
- Full Licence (Car)
- Full Licence (Bike)
- Heavy Vehicle Licence
- Do not have a Driving Licence

5) What type of a car do you drive?
- Convertible
- Coupe
- Hatchback
- People mover
- Pickup truck
- Sedan
- Sports Car
- Station Wagon
- SUV (Sports Utility Vehicle)
- Ute/Tray
- Van
- Wagon
- Other
- I do not drive a car
Telematics is a combination of positioning, telecommunications and information technologies for a range of services for road users.

6) Are you considering buying a GPS car navigation product?
   ○ Yes, in the near future
   ○ No, not in the near future
   ○ Yes, if the prices drop considerably
   ○ No, I am not interested at all

7) If telematics services are offered would you consider subscribing?
   ○ Yes, only to the ones offered FREE of charge
   ○ Yes, and would even consider paying for other value added services
   ○ No, I am not interested as they can distract me while driving
   ○ No, I am not willing to subscribe to any telematics service

8) How often do you drive out of your city of residence?
   ○ More than once per week
   ○ More than once per month
   ○ Don't travel out of city too often
   ○ Prefer not to disclose

9) If you get lost in an unknown area while driving, would you
   ○ Ask locals for direction or stop at a petrol station
   ○ Rely on your instincts
   ○ Use the telematics equipment installed in your car to find out where to go
   ○ Call somebody you think can direct you
In Pay-as-you-drive insurance, a GPS device fitted to the car transmits your location to the insurer. The premium is calculated based on how much you drive and promises potential savings for consumers. This concept would bring fairness to insurance where traditionally safe drivers of one class pay for claims of risky drivers of the same class.

**Privacy Threats**

Unintentional transmission of a lot of data to the insurer, e.g.

- How fast you accelerate
- How hard you brake
- How often you go above the speed limit

This data might be used to calculate premiums without our knowledge. The insurer knows what you were doing just before an accident, but they wouldn't use information like that against you. Would they?

10) If a rewards program, similar to FlyBuys or Credit Card Rewards, is offered where one gets rewarded to disclose precise location information, how would you respond?

- Would subscribe to such a program and receive incentives
- Would not subscribe given the potential for harm of privacy/unsolicited marketing material

11) Current Pay-as-you-drive insurance offers fairness and cost savings to consumers but it is not privacy preserving. If there are new privacy preserving insurance products on the market, which one would you choose?

- Fairer premiums, highest privacy but higher setup costs
- Fairer premiums, moderate privacy but with medium setup costs
- Fairer premiums, lowest privacy and lowest setup cost
- Not interested due to privacy reservations
- Not interested, as I am happy with current insurance
12) If you are on the road during working hours, would you be happy to reveal your location to (and reciprocally get their location) [check all that apply]

- Your peers at work
- Your boss
- Your team of employees that report to you at work
- Your friends
- Your family (spouse/partner/parents/kids)

13) If you are on the road after hours on a weekday, would you be happy to reveal your location to (and reciprocally get their location) [check all that apply]

- Your peers at work
- Your boss
- Your team of employees that report to you at work
- Your friends
- Your family (spouse/partner/parents/kids)

14) Would you like to disclose your location on weekends to (and reciprocally get their location) [check all that apply]

- Your peers at work
- Your boss
- Your team of employees that report to you at work
- Your friends
- Your family (spouse/partner/parents/kids)
You're Done!

Thank you for filling out the survey!

You may close the browser button now to finish the survey or,

Click here to log out and restart the survey.
Appendix B

IGNSS Conference Survey

Location Privacy Survey
~ Instructions & Informed Consent ~

You are invited to participate in the survey "Location Privacy and Mobility Pricing". You are selected as a possible participant in this study because of your knowledge and interest in 'Geo-Information'. The findings of this research would help in designing privacy-aware transport telematics applications.

The survey is only 6 pages long (incl this cover page) and takes an average of 15 minutes to complete. The survey contains four sets of questions seeking your opinion about three themes: (1) Telematics and GPS, (2) GPS-based Insurance and (3) Electronic Toll Collection. Every section starts with a picture related to the section followed by a general introduction of the theme.

Participation in this research is entirely voluntary. You can decline to participate without having to give a reason and without consequence. The survey is entirely anonymous - no personally identifying information is collected.

If you have any questions about this research or want access to the research report, please email Usman Iqbal at m.iqbal@student.unsw.edu.au.

Please note the following definitions used in this survey:

- "Telematics" = A combination of positioning, communications and computing technologies in the vehicle to provide value added services to motorists, like route navigation, weather reports, emergency response, vehicle diagnostics.
- "Mobility Pricing" = Mobility pricing is the use of technology to charge a fee for using road infrastructures, such as toll, congestion charging, GPS-based insurance.
- "Location Privacy" = A type of information privacy, where the mobile users claim control of the location data and its use.

How do you return the survey?

Upon completion of the survey please hand it over to the postgraduate students at the exit or alternatively leave it at the registration desk outside 'Mathews A'.

Ethical approval and declaration of interests: The ethical aspects of this research have been approved by the University of New South Wales Human Research Ethics Advisory (HREA). Ethics Approval #08/2006/35. If you have any complaints or reservations about any ethical aspect of your participation in this research, you may contact the Ethics Secretariat, The University of New South Wales, SYDNEY 2052 AUSTRALIA (phone 9385 4234, fax 9385 6648, email ethics.sec@unsw.edu.au).
# Section A: General questions about Telematics and Geo-information

Telematics is a combination of location/position, computing and communication technologies to provide a range of services to motorists, as shown in the picture.

**Instructions:**
The first section asks you some questions about GPS and telematics systems.

For questions that have value(s), circle the number(s) that best describes your situation.

For questions that have an intensity scale, ranging from 1-10, circle the number that best expresses your feeling about that question.

---

1. Do you have a GPS/GPS-enabled device?  
   Yes | No

2. If you answered 'No', to question 1, on a scale of 1-10, how interested would you be in acquiring one?  
   
<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

3. On a scale of 1-10, how familiar are you with telematics services such as Holden Assist, General Motors' Onstar, or Toyota's Link?  
   
<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

4. If these services are made available to all motorists, on a scale of 1-10, how interested would you be in subscribing to such services?  
   
<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

If No, why not? 

5. People may be tracked using telematics and GPS technologies. Evaluate this statement on a scale of 1-10?  
   
<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

6. On a scale of 1 to 10, how concerned are you about 'secondary uses' of location with tracking technologies?  
   
<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Section B: GPS-based Insurance

Description:
1. Telematics device fitted in the vehicle
2. GPS Satellite signals used to log periodic locations of the vehicle
3. GPS logs stored in the vehicle
4. The telematics system uses the GSM network to send GPS logs to insurer
5. Insurer generates invoice for insurance premium based on this data

GPS-based insurance uses telematics technology to calculate total travelled distances by the vehicle. It also takes into account when and under what weather conditions the vehicle was used. This information is used to more accurately charge premiums.

Advocates of this technology believe it provides reduction of premium payments by the average motorist, because you only pay for what you utilise. Secondly, it would make motor insurance more affordable.

Critics of this technology say that there may be privacy issues as a result of disclosure of highly-accurate GPS data to the insurance provider. In this section we seek your candid responses to the concept of GPS-based insurance.

For questions that have value(s), circle the number(s) that best describes your situation.

For questions that have an intensity scale, ranging from 1-10, circle the number that best expresses your feeling about that question.

1. Were you aware of such a product before?
   
   Yes | No

The following subsection seeks your opinion about three design alternatives for GPS-based insurance pricing; there is a trade-off between setup costs and the granularity of location disclosure.

Scenario 1: Full GPS log disclosure

2. This proposed system would work as explained in the picture in the introduction. A telematics system would be fitted to the vehicle, which continuously logs positional data and periodically uploads all the points to the insurance server. On a scale of 1-10, how interested would you be in subscribing?

<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

3. If your response is between 1 to 5 for the above question, please select a reason below?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Happy with current insurance</td>
<td>Privacy issues</td>
<td>Other</td>
</tr>
</tbody>
</table>

If you chose other, please specify here: ............................................

4. There may be initial setup costs for installing and configuring the hardware into your vehicle. How much are you willing to pledge to for its installation?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want this device free</td>
<td>Less than $50</td>
<td>$50 to $100</td>
<td>$150 to $150</td>
<td>$150 to $200</td>
<td>$200 to $250</td>
<td>$200 and over</td>
</tr>
</tbody>
</table>
Scenario 2: Moderate GPS log disclosure (aggregated)

5. In an effort to minimise location disclosure, the device fitted in the vehicle in Scenario 1, would be extended to aggregate the positional data, and only send this aggregate to the insurance provider. The same premium reduction applies to this case too. On a scale of 1-10, how interested would you be in this type of product?

<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

6. If your response is between 1 to 5 for the above question, please select a reason below?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Happy with current Insurance</td>
<td>Privacy Issues</td>
<td>Other</td>
</tr>
</tbody>
</table>

If you chose other, please specify here: 

7. For the aggregation computations to be performed on-board, the device would be extended, how much are you willing to pledge to such a device?

<table>
<thead>
<tr>
<th>I want this device free</th>
<th>Less than $50</th>
<th>$50 to $100</th>
<th>$100 to $150</th>
<th>$150 to $200</th>
<th>$200 to $250</th>
<th>&gt; $200</th>
</tr>
</thead>
</table>

Scenario 3: No GPS disclosure (computations on-board)

8. In this type of GPS-based insurance, all the payment computations would be performed on the on-board device. The original device would be extended significantly to cater to this option. No disclosure of location data is performed and insurance provider only gets information about premium receivable from its patron. On a scale of 1-10, how interested would you be in such a product?

<table>
<thead>
<tr>
<th>Not</th>
<th>Highly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

9. If your response is between 1 to 5 for the above question, please select a reason below?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Happy with current Insurance</td>
<td>Privacy Issues</td>
<td>Other</td>
</tr>
</tbody>
</table>

If you chose other, please specify here: 

10. The original device would be significantly extended to calculate premiums on-board. How much are you willing to pledge to this device?

<table>
<thead>
<tr>
<th>I want this device free</th>
<th>Less than $50</th>
<th>$50 to $100</th>
<th>$100 to $150</th>
<th>$150 to $200</th>
<th>$200 to $250</th>
<th>&gt; $200</th>
</tr>
</thead>
</table>
Section C: Electronic Toll Collection

Description:
1. Motorist pre-authorizes toll company to charge toll fees electronically.
2. A unique RFID E-tag transponder is attached to the windscreen.
3. At the toll gantry the vehicle and motorist are identified based on this identifier.
4. The system processes the toll fee and sends a bill to the motorist at each billing cycle.

1. Are you aware that all tolled roads in NSW would go 'cashless' in the near future?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

2. If a critic says, "With cashless tolling, it would be no longer possible to travel anonymously on tolled roads". Evaluate this statement on a scale of 1-10:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Rate the following three systems in terms of accuracy. Give each of them a distinct number between 1-3. (1 highly accurate...4 less accurate)

<table>
<thead>
<tr>
<th>Mobile Phone Positioning</th>
<th>Electronic Toll Records</th>
<th>GPS logs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. If a critic says, "The storage of patrons' historical toll data, even after payment processing is a cause of concern". Evaluate this statement on a scale of 1-10:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. If you were told that a cashless toll system exists, which is also anonymous, how interested would you be in it as compared to traditional unique identifier E-tags?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. If there are two payment methods available for the aforementioned anonymous option, which would you prefer? Pre-paid (pay before use, making sure sufficient credit available) or post-paid (settle with provider periodically)?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-pay</td>
<td>Post-pay</td>
<td></td>
</tr>
</tbody>
</table>

7. To avoid any misuse of positional data in the future, rate the following in terms of effectiveness. Please write a number between 1 to 4 for the following and provide a distinct number in all fields (1 highly effective...4 less effective).

<table>
<thead>
<tr>
<th>Targeted legislation</th>
<th>Industry code of practices</th>
<th>Privacy policies</th>
<th>Privacy-respecting technology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Section D: Some questions about you (Demographics)

In this section we ask you to answer some questions about yourself. For the following questions, circle the number(s) that best describes your situation.

1. **Gender:**
   - 1 Male
   - 2 Female

2. **Age:**
   - 1 Younger than 21
   - 2 21-30
   - 3 31-40
   - 4 41-50
   - 5 51-60
   - 6 60 or older

3. **Type of Licence:**
   - 1 Learners Licence
   - 2 Provisional (P1)
   - 3 Provisional (P2)
   - 4 Full Licence
   - 5 Heavy Vehicle
   - 6 Learner Rider
   - 7 Provisional Rider
   - 8 Full Rider

4. **Type of Vehicle:**
   - 1 Small Car
   - 2 Intermediate
   - 3 Full Size
   - 4 Luxury
   - 5 Sports Car
   - 6 4WD
   - 7 Other
   
   *If you chose other, please specify here: ________________________________*

5. **Education:**
   - 1 High School
   - 2 TAFE
   - 3 University Diploma/Cert
   - 4 University Bachelors
   - 5 Postgrad Diploma/Cert
   - 6 Master's Degree
   - 7 Doctorate
   - 8 Other
   
   *If you chose other, please specify here: ________________________________*

6. **What is your profession/occupation:**

7. **What level of seniority and authority do you have in your organisation?**
   - 1 Towards the bottom
   - 2 Around the middle
   - 3 Towards the top
     
     *e.g. front line worker, middle level manager, senior executive*

8. **Approx. salary:**
   - 1 Less than $20,000
   - 2 $20,000 to $39,999
   - 3 $40,000 to $69,999
   - 4 $70,000 to $99,999
   - 5 $100,000 to $149,999
   - 6 $150,000 to $250,000
   - 7 More than $250,000

---

_A Survey of Privacy and Vehicular Technologies: School of Surveying and Spatial Information Systems, University of New South Wales_
Références


Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd. (2001). High Court of Australia. 63.


of the ACM. 31(5), 498–512.


www.ietf.org/html.charters/geopriv-charter.html


Onstar. (2008). OnStar by GM - Onstar Technology, Global Positioning System and GPS Maps. Consulté le 20th September,


International Symposium on Geoinformation. 27-29 September, Penang, Malaysia. (Invited Paper)


Transport Reviews, 5(4), 301–324.

the electronic tolling industry. Strathfield, NSW, Australia: Standards 
Australia International Ltd.

Worth, Tex.: Harcourt. (William Pitt, as quoted in this book)

subaru.g-book.com/pc/


Synnes, K., Nord, J., & Parnes, P. (2003). Location Privacy in the Alipes Plat-
tform. Paper presented at the 36th Annual Hawaii International Conference 
on System Sciences (HICSS’03).

Tetsusaki, K. (1994). High security electronic toll and traffic management and 
road pricing system using encrypted messages and personal identity num-
ber. In Proceedings of the IEEE Vehicle Navigation and Information Sys-
tems Conference (p. 695-698).

Channel Online)

sur http://www.nytimes.com/2000/12/03/nyregion/new-plans-for 
e-zpass-would-include-airport-parking.html?n=Top/Reference/


Wainright, R. (2007). Father and son stick to guns to prove radar


