The Intelligent Number Plate System: protection or violation of motorists' privacy?

Erin Hommes

Department of Information Science
School of Information Technology
University of Pretoria
Tel: 012 420 2230
Email: erin.hommes@up.ac.za

Marlene Holmner

Department of Information Science
School of Information Technology
University of Pretoria
Tel: 012 420 5215
Email: marlene.holmner@up.ac.za

Marietjie Schutte

Department of Information Science
School of Information Technology
University of Pretoria
Tel: 012 420 2963
Email: marietjie.schutte@up.ac.za

ABSTRACT

A number of ethical issues have come under the spotlight with the proposed implementation of an Intelligent Transport System (ITS), known as the Intelligent Number Plate System (INPS), to be used in the Open Road Tolling (ORT) system designated for certain Gauteng roads in 2011. The project was first initiated in 2006, with full-scale implementation scheduled for 1 January 2008. It was, however, postponed to January 2009 and later to April 2010. When this deadline could not be met, it was postponed to October 2010 and subsequently to October 2011.This research investigated some of the ethical issues related to the surveillance that motorists will experience each time they utilise the impacted roads. This surveillance will be made possible via technologies that include closed-circuit television and radio frequency identification tags. When considering the possible vulnerability of such technologies, it is important to make motorists aware

of the authorities' responsibility to protect any identifying information, as well as the potential effect these systems may have on motorists' right to privacy. These rights will be illustrated through an analysis of South African legislation and its relation to the INPS. International examples of ITSs were investigated to determine the possible benefits and challenges related to the implementation of the INPS. In order to supplement the literature research findings, a pilot study was conducted to assess the public perception of the privacy challenges associated with the INPS. The research findings indicated that there was cause for concern related to the ethical issues involved in the implementation of such a system in a South African context.

KEYWORDS

Information ethics, Intelligent number plate system, Intelligent transport systems, Radio frequency identification, South African legislation.

1. INTRODUCTION

As technology advances and becomes more intrusive in our public and private lives, unauthorised access to an individual's personal information becomes an ethical challenge, especially when care is not taken to apply security measures to maintain confidentiality. In this respect, information ethics, a branch of applied ethics (Bynum 2008), is concerned with the ethical implications of the usage of technology, informational objects and processes that compromise moral conduct and violate the privacy of individuals' personal details (Floridi 2006:38). Furthermore, Britz (1996) pointed out that the main ethical impacts of technology were the accessibility/inaccessibility of information and the ability of the user to exercise control over it. It is, therefore, important to understand which ethical and moral considerations apply when employing technology, and specifically, information systems to use and distribute information.

The Gauteng Provincial Government earmarked 1 December 2010 (Gauteng Provincial Government 2010:31) for the proposed implementation of the Intelligent Number Plate System (INPS). However, very little progress had been made up until September 2011. This system is being developed by the Gauteng Department of Roads and Transport as part of a smart crime-fighting initiative aimed at putting an end to the duplication of number plates frequently used in motor vehicle theft and other illegal practices. The INP system will make it possible to undertake a roll call of all vehicles in Gauteng to ensure all are properly registered and licensed, as well as assist in improving revenue collection due to improved vehicle identification (AA Mobility Magazine 2010:63; Gauteng Provincial Government 2010:31; Rasool 2010). The INPS is to represent one component of an Intelligent Transport System (ITS), an umbrella term used to describe new in transit technologies for security, traffic control and prompt response by emergency services, in an attempt to help save money, time and lives (Casal 2005:66; Chattaraj et al. 2009:40; Deaking et al. 2009:1). The INPS will make use of closed-circuit television

(CCTV) cameras, Variable Message Signs (VMS) and Radio Frequency Identification (RFID) tags as a means of tracking and surveillance of motorists on Gauteng national roads (SANRAL 2010). For the purposes of this research, the investigation was limited to the context of the N1i.

The purpose of the research was to promote the debate of responsible information use, and to create an overall awareness of the possible use and/or misuse of recorded personal information. The value of this research study lies in the currency of the theme. It is envisaged that the INPS may cause privacy concerns for motorists, and based on this, an investigation into these concerns was conducted.

2. RESEARCH METHODOLOGY

The primary research paradigm was a qualitative literature review. The researchers explored the issues pertaining to information ethics, privacy, South African legislation and ITS implemented around the world, by means of a literature review. Furthermore, this enabled the researchers to understand phenomena such as the benefits and challenges of ITS, and assisted in determining the most recent thinking about privacy and information privacy.

The secondary methodological approach was quantitative in nature. A pilot study was conducted to determine individual feelings and thoughts regarding privacy issues that may affect the successful implementation of the INPS. The pilot study questionnaire, containing 20 closed-ended questions, was distributed to obtain data on the participants' understanding of the potential ethical implications of the INPS.

Participant selection constituted a non-probability, convenience-sampling approach. This approach was selected due to the convenience of access to the participants as well as their proximity to the researchers (Castillo 2009).

On 16 April 2010, the pilot study questionnaire was issued to a group of 156 second-year students studying information ethics at the Hatfield campus of the University of Pretoria. The selection of this location was based largely on accessibility to the studentsii and the similarity between the research theme and themes covered in their semester course. Babbie (2008:204) illustrated the reasoning behind why the research could only be regarded as a pilot study, explaining that "[u]niversity researchers frequently conduct surveys among students enrolled in large lecture classes. The ease and frugality of this method explains its popularity, but seldom produces data of any general value." This method may, however, be considered useful in pre-testing a questionnaire, which was the researchers' intention with this research. With the insights gained from the pilot study, the researchers would be able to generate a more comprehensive questionnaire together with a more focused evaluation of the involved target group for further research.

3. BACKGROUND TO THE STUDY

3.1 INTERNATIONAL EXAMPLES OF ITS

As mentioned before, ITS is an umbrella term for smart transit systems such as the INPS. Examples of the international application of ITS include Automatic Number Plate Recognition (ANPR), currently in use in Germany, Hungary, the United Kingdom, and the United States (Wikipedia 2010). Radio Frequency Identification (RFID)-enabled license plates are also used in the United Kingdom, Bermuda, Brazil, China, Dubai, India and Mexico (Bacheldor 2008). These systems are used for vehicle identification, tracking of traffic flow, collection of driver information, automatic tolling, and congestion taxing (Transport for London 2010).

3.2 THE INTELLIGENT NUMBER PLATE SYSTEM

On 10 February 2010, General Notice 333 of 2010 of the Gauteng Provincial Gazette Extraordinary Number 13 was released, detailing the implementation of the Gauteng License Mark System under the National Road Traffic Act (No 93 of 1996). This system is otherwise known as the Intelligent Number Plate System (INPS).

According to the notice, the INPS consists of an embossed aluminium number plate, displaying two letters, two numbers, and two letters following, as depicted in figure 1.

Figure 1

Each plate will show the Gauteng logo, as well as a two-dimensional barcode (depicted in figure 2) and a unique identification code transmitted by an RFID tag. These tags contain small wireless radio transmitters. Each tag has a unique identification number, and is tuned to a specific frequency. As the tag receives a signal from an interrogating reader, it relays the identification information back to the transmitter (Pfleeger and Pfleeger 2009:639). An authorised service provider permanently attaches the tag, with dimensions of 30mm x 44mm x 1.9mm, by means of a secure process.

Figure 2

3.3 THE POTENTIAL BENEFITS OF THE INPS

Based on an analysis of available literature regarding the benefits of ITS and INPS, the following potential benefits were identified for a South African context (Chattaraj et al. 2009:40; Deaking et al. 2009:29; SANRAL 2010):

- Reduced congestion through smart traffic management, such as assigning priority traffic and the use of VMS.
- Improved incident management, leading to a more efficient accident response time.
- A reduced incidence of crime due to a decreased number of fraudulent license plates, as well as fewer incidents of car and identity theft.

3.4 THE POTENTIAL CHALLENGES OF IMPLEMENMTING THE INPS

Implementation of an ITS that contains location tracking technology can be a double-edged sword (Laudon and Laudon 2004:126). It can be a source of many benefits as discussed above, but can also create new challenges, including:

- Extensive deployment costs to be incurred, with an estimated launching cost of R25 million allocated by the Gauteng Road and Transport Budget Plan for 2010/11 (Nkosi 2010).
- Liability concerns with regard to the violation of rights, such as the right to privacy, as outlined by the South African Constitution.

- Differing interests of motorists (data owners), and SANRAL (data retriever) in terms of the value of the information collected (Casal 2005). At this stage, there is not a great deal of clarity on how motorists' information will be stored.

3.5 RFID CONCERNS

Pfleeger and Pfleeger (2009:640) discussed additional security and privacy limitations pertaining to RFID technology used in an ITS, namely:

- The ability to track individuals wherever they are located.
- The ability to access sensitive data about individuals.
- Malfunctioning of the RFID reader resulting in a system failure or glitch leading to mistaken identification.

The intention to circumvent RFID technologies may also create increased opportunities for contravening the law (Laudon and Laudon 2004:126).

Many individuals, who do not wish to have their movements tracked, may employ several illegal privacy-restoring tools, such as: (Pfleeger and Pfleeger 2010:640):

- "blasting" – the process of disabling a RFID tag;
- "reprogramming" – the user altering the tag so that it emits different identification information;
- "encrypting" – the user selectively making the signal available; and
- "blocking" – the user shielding a tag to block access from the reader.

As discussed previously, many countries have implementated ITS in one form or another, many including RFID tracking. On 11 March 2008, the Federal Constitutional Court of Germany ruled that the ITS system utilised in Germany violated motorists' right to privacy by tracking and recording their daily travelling habits (Das Bundesverfassungsgericht 2008). This demonstrated an already growing dissatisfaction with transportation surveillance and tracking systems, and the challenges faced in protecting privacy.

3.6 PRIVACY AND INFORMATION PRIVACY

Privacy has often been described as the "right to be let alone" (Shank 1986:12; Stair 1992:635; Rauhofer 2008:187). The right to privacy includes the control exerted over external influences and personal information, such as the public display of identity (Neethling et al. 1996:36; Kizza 2010:90). Another important aspect of privacy, raised by Britz (1996) states that "the legal right to privacy is constitutionally protected in most democratic societies. This constitutional right is expressed in a variety of legislative forms."

According to Gupta (2006:424), information privacy can be described as "the individual's ability to control the circulation of information relating to him/her". He further describes information privacy as the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".

3.7 IDENTITY, PERSONAL INFORMATION AND PRIVACY IN A DIGITAL ENVIRONMENT

Halperin and Backhouse (2008:3) discussed five different perspectives with regard to identity, including:

- tensions
- themes
- application areas
- research focus, and
- disciplinary approaches.

For the purpose of this research, only the first two were considered, namely tensions and themes.

i. TENSIONS

The recording and accessibility of personal information via technology are creating tensions between security and privacy. For security reasons, governments may implement systems which, although intended to enhance protection, in fact may violate individuals' privacy (Bhattacharya and Gupta 2005:120). This relates directly to possible privacy concerns that the implementation of the INPS will have for motorists.

Similarly, the tensions between convenience and intrusiveness imply a paradoxical situation, as emerging technologies may offer new and convenient services to the public, but often run the risk of causing intrusion, either from over-use by organisations, or from illegal use by those who obtain users' information illegally. With regard to the INPS, the convenience offered by the system, such as prompt emergency response, crime prevention and traffic warnings (SANRAL 2010), can be over-shadowed by privacy violations caused by inadequate security measures and unauthorised access.

Interoperability refers to integrating various identification management systems, eliminating the need for users to provide the same identification information multiple times, when utilising various systems (Backhouse 2006:568). This raises serious concerns relating to the security measures that will be needed to protect information in the INPS repository. These concerns not only relate to the repository but also to other systems that the INPS may possibly integrate with, such as the National Traffic Information System (eNatis) (SAIT News 2010).

ii. THEMES

One way in which privacy can be protected in an environment of intrusive technologies, is by means of digital identity management. This can be broadly defined as the management of or interaction between a user and his/her identification information that is stored digitally (Gutierrez and Feigenbaum 2006:5). Technologies employed in user-centric digital identity management systems include smartcards, biometrics and RFID chips (El Maliki & Seigneur 2007:12). However, systems that protect such identity are vulnerable to changes in power structures, such as changes in data ownership and custodianship, which may lead to changes in roles, responsibilities and risks (Rannenberg et al. 2009:8).

In relation to the INPS, further research by authorities regarding these issues will be necessary to ensure the long-term integrity and protection of personal information. In terms of digital identity, an inadequate management system could result in severe misrepresentation. An example of this is the current eNatis system in use. According to Carte Blanche's Devi Govender (2010), an investigation was conducted by Carte Blanche into the increasing incidents of cloned driver's licenses in South Africa. The investigation determined that the eNatis system does not have adequate digital identity management and security features, and with a history of corruption among licensing authorities, it was open to exploitation and fraudulent activity. This failure in the current system emphasises the need for a system such as the INPS to implement stronger measures to prevent and reduce fraud. Furthermore, changes in power structures as a result of general elections, for example, can jeopardise the integrity of the INPS. Such power structure changes could result in focus and policy alterations and a shift in priorities, such as allocation of funding. These changes may impact either negatively on the protection of information in the INPS repository, or positively if a more serious stance is taken against fraud and corruption relating to vehicles (Govender 2010).

B. SOUTH AFRICAN LEGISLATION RELATED TO INFORMATION PRIVACY AND INFORMATION PROTECTION

i. THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA (ACT NO 108 OF 1996)

Privacy, as a basic human right, is protected by the South African constitution in the following sections:

- Section 14 states:

  Everyone has the right to privacy, which includes the right not to have:

  (a) their person or home searched;

(b) their property searched;

(c) their possessions seized; or

(d) the privacy of their communication infringed.

- Section 10 states:

  Human dignity – Everyone has inherent dignity and the right to have their dignity respected and protected.

Section 10 of the Constitution directly addresses what Kizza (2010:90) believes privacy to be – the core of human dignity. With regards to sections 10 and 14 of the Constitution, the INPS may well be treading a very fine line, as it could risk contravening both human dignity and the right to privacy. By tracking a motorist's movements or monitoring him/her via surveillance and recording personal information, the motorist's privacy is at risk, along with his/her human dignity. According to Kizza (2010:91), an individual's human dignity is not being respected and protected when he/she has no control over what personal information is disseminated.

To ensure individuals' constitutional right to privacy and human dignity with regard to information, the Protection of Personal Information Bill was introduced. The bill is aimed at protecting South Africans "against the unlawful collection, retention, dissemination and use of personal information."

ii. THE PROTECTION OF PERSONAL INFORMATION BILL (NO 9 OF 2009)

This bill was drafted in order to "regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests" (South Africa 2010).

Currently, the bill only serves as a guideline for information protection. Once promulgated as an act, motorists travelling on the N1 highway will benefit from this forthcoming legislation, as it demands that personal information captured in a repository be adequately protected against unauthorised access and misuse. Furthermore, the legislation provides a mechanism, in the form of a regulator, for resolving disputes arising from automated decision-making systems, such as automated tolling and fining.

Although this legislation also makes provision for the necessity of codes of conduct and protection against unsolicited electronic communication, these aspects are more suitably covered by the Electronic Communications and Transactions Act.

iii. THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT (NO 25 OF 2002)

The ECT act impacts upon the electronic communication of information, and should not be regarded in isolation from other legislation related to information protection matters. It also refers directly to section 14 (d) of the constitution. A key issue addressed in the act relates to the protection of an individual's personal information and critical data (Michalsons 2005:2).

Two chapters of the ECT act have direct relevance to this article, namely chapter VIII and chapter IX:

- Chapter VIII addresses personal information and privacy protection and establishes a voluntary management of personal information. Collectors of personal information, in this case SANRALiii and the Gauteng Provincial Government, should subscribe to a set of universal data protection principles. Unfortunately, according to this act subscription to these principles is voluntary, and thus poses a potential risk in terms of violating the privacy of personal information recorded by the INPS.
- Chapter IX embarks on the protection of critical data. If compromised, such data poses a risk to the economic or social wellbeing of South African citizens. Through identity theft or fraudulent activities the economic and social wellbeing of motorists can be affected negatively by the directives of the INPS. In the case of the INPS, the authorities must implement the necessary procedures and technological methods to ensure the integrity and protection of personal information within the INPS repository.

From this discussion, it can be inferred that the privacy of information is already protected by various aspects of South African legislation. ITSs such as the INPS should not contradict the rights and responsibilities stipulated in the abovementioned legislation.

C. AN INTERPRETATION OF PRIVACY CONCERNS RELATED TO THE INPS

Having discussed the benefits and challenges of INPS, personal information and privacy in a digital environment, as well as relevant South African legislation, the researchers now focus on privacy concerns the INPS could potentially bring about.

Alex van Niekerk (personal communication 2010iv), the project manager at SANRAL, mentioned that an average of 200 000 motorists are recorded travelling along the N1 highway on a daily basis. The AA Mobility Magazine (2010:63) confirms this statistic, indicating that there were an estimated 180 000 trips on the highway in both directions (north and south) on any given day. When the INPS is in effect, the implication is that these motorists may have their personal information communicated to a government

managed database on a daily basis. This includes information regarding aspects such as location, type of vehicle and daily travelling habits.

The control of these aspects relates to Durlak's two categories of privacy rights (cited in Kizza 2010:90), namely the control of external influences and the control of personal information. The first category describes factors such as solitude (the right to be let alone), anonymity (the right to have no public personal identity) and intimacy (the right not to be monitored). At a general privacy level, the implementation of the INPS would affect the motorist in relation to all three these factors. Motorists would not be let alone on their daily journeys, they would have a public identity on a central database accessible by SANRAL, and their movements would be monitored through the use of radio frequency transmitters in their license plates.

Kizza (2010:91) refers to the second category as "the right to control one's personal information including methods of dissemination of that information", highlighting the link between information and the privacy thereof. As information privacy is the right to determine how information relating to a person is communicated, one of the biggest challenges of the INPS is how to deal with the exposure of this personal information, should the INPS be compromised in any way.

6. PILOT STUDY FINDINGS

As outlined in the research methodology, a pilot study was conducted to minimise possible processing errors in future research. While the circumstances for the study were not ideal, it did produce resultsv worthy of consideration. This section outlines the results in four themes for ease of analysis:

- Demographics of population
- Transport status
- Privacy: perceptions and acceptable risks
- Respondents' perceptions of the INPS.

A. DEMOGRAPHICS OF THE PARTICIPANTS

The following questions relate to the demographics of the participants of the pilot study, focusing on age and gender.

Age and gender

The fact that most respondents were between the ages of 20 and 21 illustrates the limitations of this research. This age group does not in any way adequately represent the entire population of motorists who will be affected by the INPS. However, as this was only a pilot study, the use of this sample group was adequate for testing perceptions

of privacy violations of systems such as the INPS. With regard to gender, the sample group was almost equally represented, consisting of 49% male students and 51% female students.

B. TRANSPORT STATUS

Of the 156 participants in the pilot study, only 38% held a valid driver's license. Of those 38% who have a valid driver's license, the majority (80% of participants) made use of a vehicle owned by a parent/guardian1.

C. PRIVACY: PERCEPTIONS AND ACCEPTABLE RISKS

Question 8: For what purpose do you believe it is acceptable to locate vehicles via a tracking device? (You may circle more than one answer to this question)

Participants were requested to provide multiple responses to this question (see figure 3). The most significant responses for acceptable use of tracking devices included:

- 85% of the participants believed that adding a tracking device to a car is only acceptable for police locating stolen vehicles.
- 71% of the participants believed that automatic locating and calling of emergency services in the case of a car accident is an acceptable reason for vehicle tracking.
- Only 1% of participants believed that it was never acceptable to track vehicles.

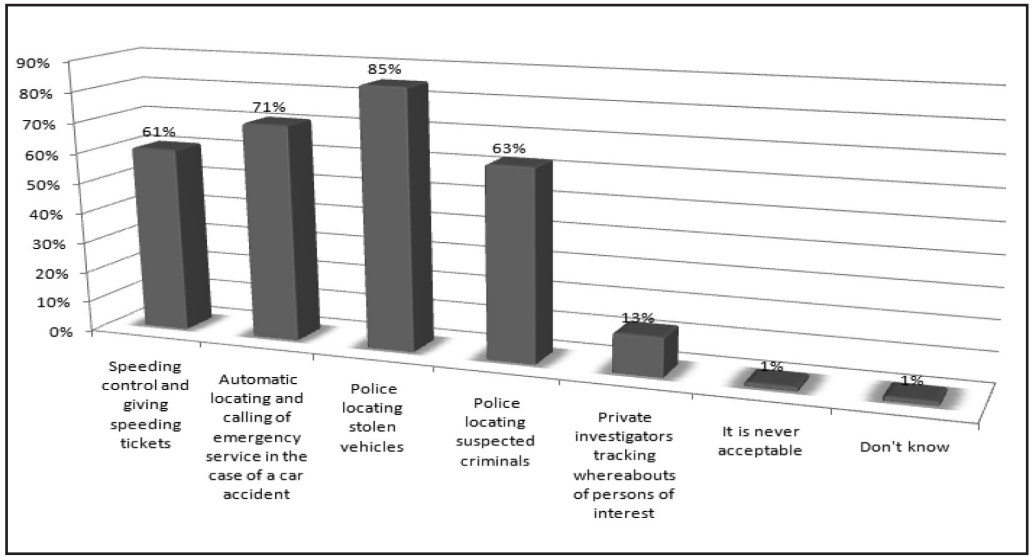

Figure 3: Indicator of acceptable reasons for installing tracking devices on vehicles.

Question 12: If you have nothing to hide you don't have to worry about security technologies such as tracking devices that may infringe your privacy.

In showing their agreement/disagreement with the statement, 40% of the respondents completely agreed and 19% partly agreed that security technologies do not infringe on their privacy if they have nothing to hide (see figure 4). While the majority of respondents agreed with the statement, a notable 17% of respondents completely disagreed that a person does not need to worry about security technologies infringing on privacy.

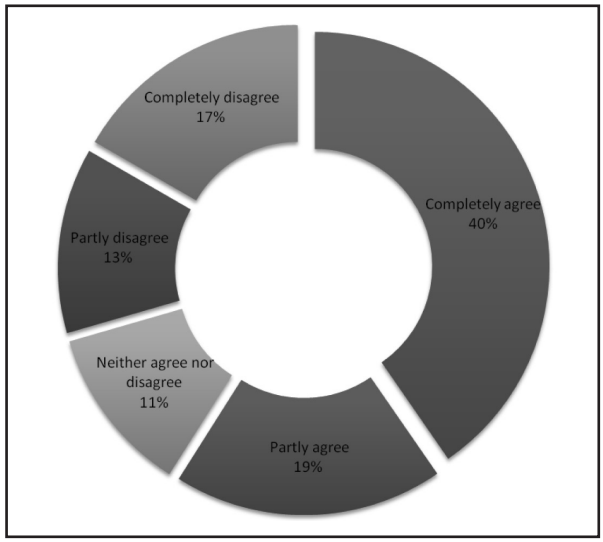

Figure 4: Indicator of concern relating to security technologies infringing on privacy.

Note: Of those who agreed (either completely or partly) with this statement, 52% held a valid driver's license. In comparison, those who agreed (completely or partly), 64% did not hold a valid driver's license (see table 1). This can be the basis for a reasonable assumption that those who do not have a driver's license feel less threatened by a system such as the INPS.

Table 1: Percentage of respondents who agree that security technologies do not infringe on privacy

	Driver's license (n=58)	**No driver's license (n=96)**
Completely agree	21	41
Partly agree	9	20
Total	**30**	**61**
Agree (%)	**52%**	**64%**

Question 13: Privacy should not be violated without reasonable suspicion of criminal intent.

Respondents seemed to react strongly to this statement, with 69% of respondents strongly agreeing with the statement, and 18% partly agreeing with it (see figure 5). Very few respondents (6%) had any feeling of disagreement with this statement.

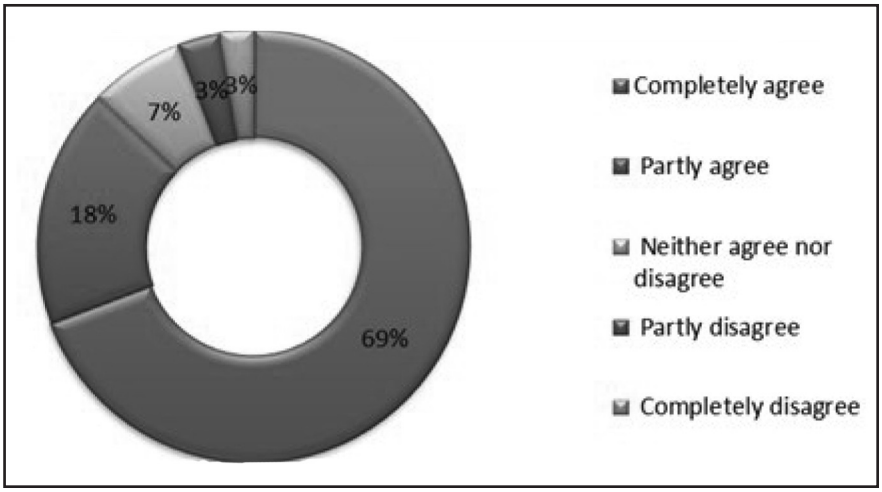

Figure 5: Indicator of whether privacy should not be violated without reasonable suspicion of criminal intent.

Question 14: It is unnerving to be under surveillance, even though you do not have criminal intent.

Similar to question 13, the response to this statement was strong, with 41% of respondents completely agreeing that it is unnerving to be under surveillance, and 29% partly agreeing with the statement (see figure 4). Once again only a small portion of respondents (14%) disagreed with this statement.

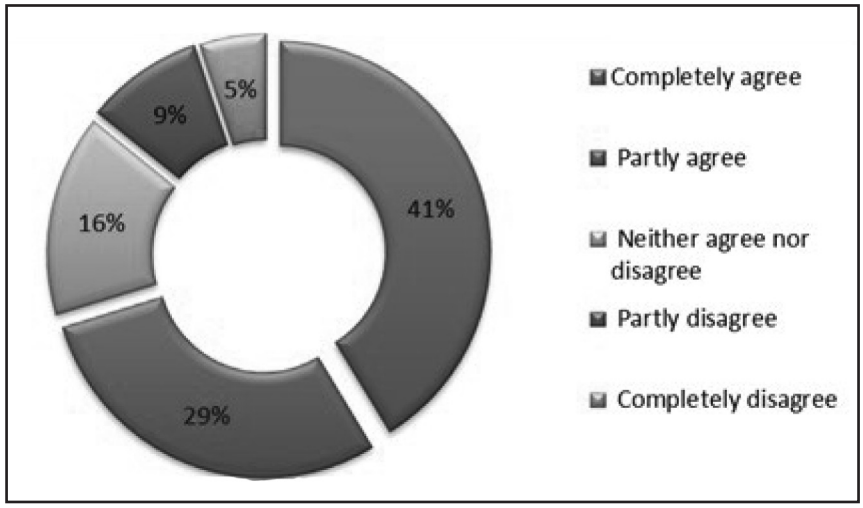

Figure 6: Indicator of discontent with being under surveillance.

When doing a cross-question analysis of the responses to questions 12 and 14, a clear contradiction emerges. The results of question 12 show that 59% of respondents agreed (completely or partly) that one should not be apprehensive about surveillance technologies if one have nothing to hide, while in question 14, 70% of respondents agreed (completely or partly) that even though one has nothing to hide, it is unnerving being under surveillance (see table 2). These students' responses contradict one another, indicating either a misinterpretation of the questions, or that some respondents apply a double standard – what may be good for others, may not good for the individual.

Table 2: Percentage of respondents who agree with question 12 and question 14

	Question 12 (n=156)	**Question 14 (n=156)**
Completely agree	63	64
Partly agree	29	45
Total	**92**	**109**
Agree (%)	**59%**	**70%**

Question 18: The possibility of locating all vehicles is privacy infringing.

The response to this statement illustrated a slightly different perspective on the respondents' beliefs on privacy infringement. The majority of respondents, 39%, only partly agreed that the possibility of locating cars is privacy infringing. This does coincide with the responses to question 8, where many respondents believed that only some of the reasons for tracking and locating cars were acceptable.

Question 16: New security technologies are likely to be abused by criminals.

The reaction to this question can be arguably symptomatic of South Africans' perception of crime and corruption. With a previously mentioned history of corruption by licensing authorities (see 3.2.2), it is not surprising that the majority of respondents completely agreed (47%) and partly agreed (25%) that security technologies are likely to be abused by criminals (see figure 5). This also supports the assumption that interception or alteration of RFID tags poses a possible challenge to the INPS, placing motorists' identification information at risk of theft and exploitation.

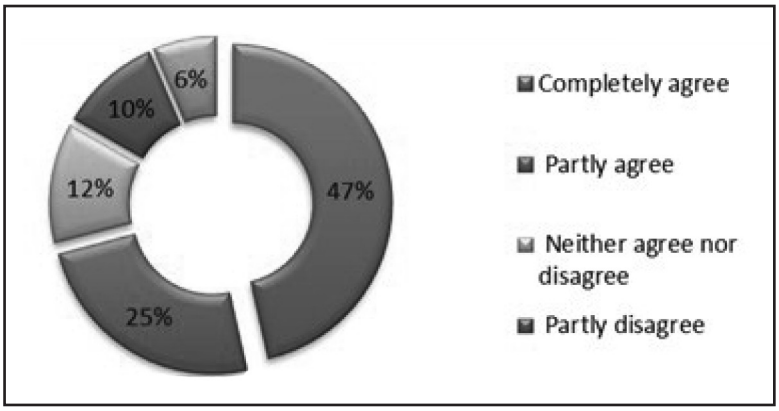

Figure 7: Perceptual indicator of abuse of security technologies by criminals.

D. RESPONDENTS' PERCEPTIONS OF THE INPS

Question 15: New security technologies are likely to be abused by governmental agencies.

47% of respondents indicated that they completely agreed with the above statement, whilst 28% partly agreed (see figure 9). Very few respondents (9%) disagreed with this statement. This indicates a perception of the use of information by government agencies, and supports the idea of misuse of information by authorities as a challenge of the INPS.

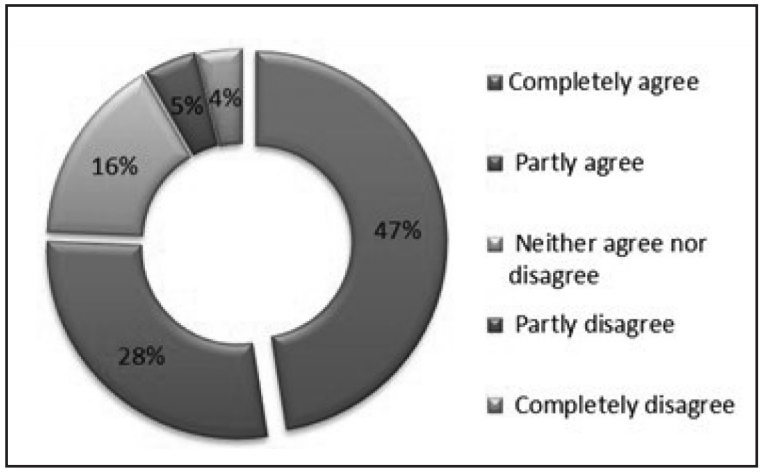

Figure 8: Perceptual indicator of abuse by government of security technologies.

In doing a cross-question analysis, it emerged that 28% of the respondents completely agreed with the statement in both question 15 and question 16. This indicates a similarity in perception of potential abuse of security technologies by both criminals and government officials.

Question 17: Should the Intelligent Number Plate System automatically be installed in all cars?

In terms of the INPS being automatically installed in all cars, 40% of the respondents replied yes, whilst 31% felt that is should be optional (see figure 9). 17% of respondents felt that the installation of such a system should be mandatory, but an option to deactivate the radio signal of the RFID tag should also be available.

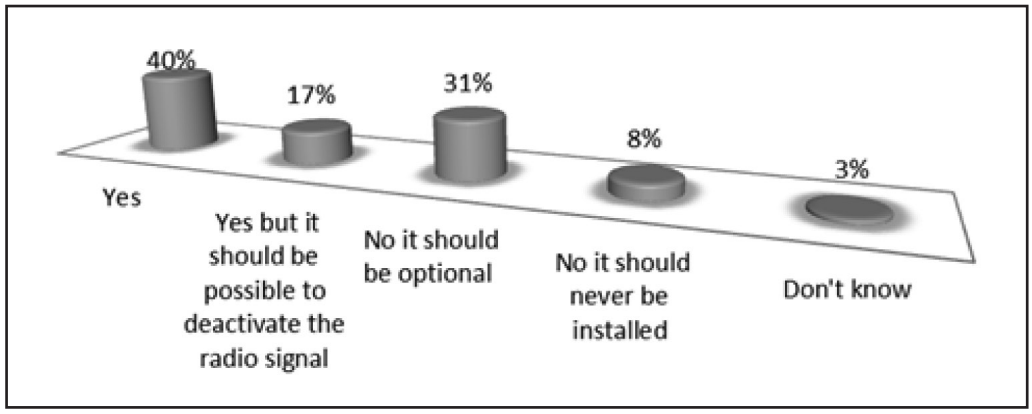

Figure 9: Automatic installation of INPS.

Question 19: The possibility of locating all vehicles is a good tool for the police in investigating and preventing terror and crime.

The largest segment of the respondents agreed completely (59%) or partly (26%) with the above statement (see figure 10). It can be concluded that most respondents have a favourable perception of the INPS, should it be utilised for crime prevention.

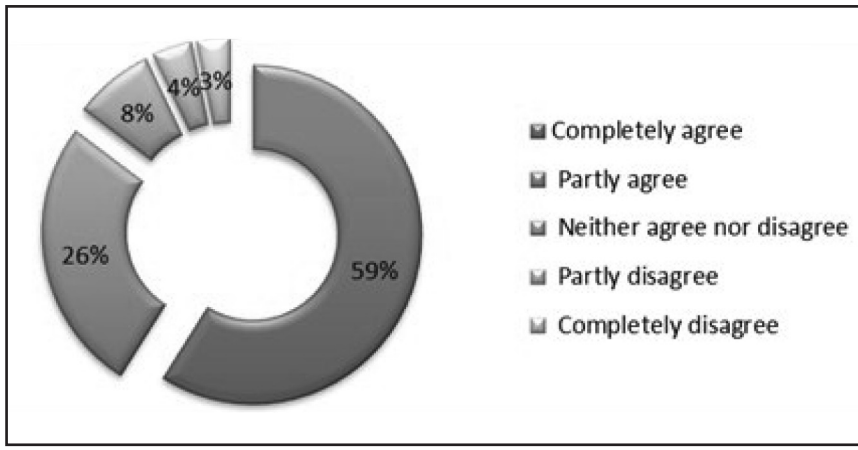

Figure 10: Indicator that locating vehicles is a good tool for police.

7. CURRENT INPS PROJECT STATUS

Since the original research conducted on this matter took place in 2010, the INPS project is still on hold for implementation in Gauteng in 2012, and currently there is no indication as to the future of the project. Conflicting reasons are given for the delay in implementation, including:

- Investigations into tender irregularities of 13 contracts linked with the entire ITS (Mail&Guardian 2011; Rasool 2011a & b).
- Auditor general investigation into non-compliance, mismanagement and irregular expenditure in the Gauteng Department of Roads and Transport (Jones 2011; Techcentral 2011).
- Lack of competition (Rasool 2011b).
- None of the proposed technology for the license plates had met the Gauteng Department of Roads and Transport standards (Rasool 2011b).
- Testing of new technologies other than RFID (Rasool 2011b).
- The demand for a national blueprint for INPS for all provinces in South Africa (Phakathi 2011; Rasool 2011a).

The numerous conflicting reports have created a great deal of uncertainty as to when exactly the system will begin roll out, and whether or not it will make use of the same technologies outlined in the original provincial gazette.

8. CONCLUSION

The INPS is one component of an ITS in the process of being implemented by SANRAL and the Gauteng Department of Roads and Transport as a means of tracking and surveillance of motorists on the N1. The system is expected to ease traffic congestion, reduce crime, and improve incident management. These benefits may be hampered by high deployment costs, and, more importantly, possible contravention of privacy and information protection rights, as outlined by legislation.

The pilot study was valuable in terms of offering insight into perceptions and beliefs of some citizens with regard to the implementation of systems such as the INPS. The pilot study confirmed that respondents recognise that the INPS could hold certain benefits, especially in respect to crime reduction, traffic management, and emergency services. However, the evidence suggests that the implementation of the INPS may be cause for concern regarding privacy issues, and there is clearly still a significant fear of mismanagement or misconduct in such a system.

In the researchers' opinion, following the reviewed literature and the pilot study, a strong perception exists that the implementation of the INPS has the potential to violate South African citizens' basic constitutional rights regarding privacy and human dignity. Further investigations into the vulnerabilities of the INPS should be conducted before the South African government goes forward with its implementation.

NOTES

1 Note: The number of participants who selected an option for the vehicle they make use of in question five (64 responses) was more than those who replied "yes" to having a driver's license in question four (56 responses). This may indicate either a lack of understanding of the question, or the possibility that some students were driving vehicles with a learner's license or without a valid driver's license, which would be a possible aspect of further study with regard to the fraud prevention aspect of the INPS.

i The N1 highway referred to throughout this article is the section of highway between Pretoria and Johannesburg.

ii At the time, the researchers were working in the Department of Information Science, University of Pretoria.

iii SANRAL has been appointed as the managing authority of the INPS by the Gauteng Provincial Government.

iv This information was received from Alex van Niekerk during a tour of the SANRAL offices in Midrand, Gauteng on 8 April 2010.

v Due to conflicting information in official government statements, press releases and notices, some of the questions in the pilot study were no longer regarded as relevant at the time of this analysis, but the results will be retained for possible future study.

REFERENCES

AA Mobility Magazine. 2010. New GP plates - when? Cape Town: Highbury Safika Media.

Babbie, E. 2008. The basics of social research. Florence, KY: Cengage Learning.

Bacheldor, B. 2008. Electronic vehicle registration picks up speed. http://www.rfidjournal.com/article/view/3945 (Accessed 23 September 2010).

Backhouse, J. 2006. Interoperability of identity and identity management systems. Data Protection and Data Security 30(9):568-570.

Bhattacharya, J & Gupta, SK. 2005. EPAL based privacy enforcement using ECA rules. Proceedings of International Conference on Information Systems Security, ICISS, Dec 2005, Kolkata, India LNCS 3803:120-133.

Britz, JJ. 1996. Technology as a threat to privacy: ethical challenges and guidelines for the information professionals. *Microcomputers for Information Management: Global Internetworking for Libraries* 13(3-4):175-194.

Bynum, T. 2008. Computer and information ethics, in Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/entries/ethics-computer (Accessed 11 August 2010).

Casal, CR. 2005. Privacy within in-car systems. *Info* 7(1):66-75.

Castillo, JJ. 2009. Quota sampling applied in research. http://www.experiment-resources.com/quota-sampling.html (Accessed 13 November 2010).

Chattaraj, A, Bansal, S & Chandra, A. 2009. An intelligent traffic control system using RFID. *IEEE Potentials* 28(3):40-43.

Das Bundesverfassungsgericht. 2008. Press releases. http://www.bverfg.de/en/press.html (Accessed 28 October 2010).

Deaking, E, Frick, K & Skabardonis, A. 2009. Intelligent transport systems: linking technology and transport policy to help steer the future. *Access* 34:29-34.

El Maliki, T & Seigneur, JM. 2007. A survey of user-centric identity management technologies. *Secureware* 21: 12-17.

Gauteng Provincial Government. 2010. Provincial Gazette Number 13 Notice 333 of 2010. Gauteng: Gauteng Provincial Government, South Africa.

Govender, DS. 2010. Cloned cars. Carte Blanche Consumer 14 October 2010. http://beta.mnet.co.za/carteblanche/Article.aspx?Id=4160 (Accessed 12 November 2010).

Gupta, GK. 2006. Introduction to data mining with case studies. New Delhi, India: PHI Learning Pvt Ltd.

Gutierrez, AJ & Feigenbaum, J. 2006. Towards better digital identity management. *Sensitive Information in a Wired World* 1-24.

Halperin, R & Backhouse, J. 2008. A roadmap for research on identity in the information society. *Identity in the Information Society* 1(1):1-17.

Jones, G. 2011. Gauteng tender flaws: "the rot is deep". http://mg.co.za/article/2011-06-15-gauteng-tender-flaws-the-rot-is-deep (Accessed 20 September 2011).

Kizza, JM. 2010. Ethical and social issues in the information age. 4th ed. New York, NY: Springer Verlag.

Laudon, KC & Laudon, JP. 2004. *Management information systems: managing the digital firm*. 9th ed. Englewood Cliffs, NJ: Prentice Hall.

Mail&Guardian. 2011. Gauteng roads paved with bad tenders. http://mg.co.za/article/2011-06-14-gautengs-hellish-roads-paved-with-good-intentions-bad-tenders (Accessed 20 September 2011).

Michalsons. 2005. Guide to the ECT act. http://www.irmsa.org.za/library/iforest/Michalsons%20Infosheet%20-%20Guide%20to%20the%20ECT%20Act.pdf (Accessed 25 November 2010).

Neethling, J, Potgieter, JM & Visser, PJ. 1996. Neethling's law of personality. Durban: Butterworths.

Nkosi, B. 2010. Roads and transport budget plans for 2010/11. Speech to the Gauteng Provincial Legislature, 18 May 2010.

Phakathi, B. 2011. Government mulls over regional number plates. http://www.businessday.co.za/articles/Content.aspx?id=147438 (Accessed 20 September 2011).

Pfleeger, C & Pfleeger, SL. 2009. Security in computing. Upper Saddle River, NJ: Prentice Hall PTR.

Rannenberg, K, Royer, D & Deuker, A. 2009. The future of identity in an information society. Hong Kong: Springer.

Rasool, F. 2010. Another delay for intelligent plates? http://www.itweb.co.za/index.php?option=com_content&view=article&id=33713:another-delay-for-intelligent-plates&tmpl=component&print=1 (Accessed 10 May 2012).

Rasool, F. 2011a. Gauteng rejects intelligent plates. http://www.itweb.co.za/index.php?option=com_content&view=article&id=43669:gauteng-rejects-intelligent-plates (Accessed 20 September 2011).

Rasool, F. 2011b. Investigation delays intelligent plates. http://www.itweb.co.za/index.php?option=com_content&view=article&id=40327:investigation-delays-intelligent-plates (Accessed 20 September 2011).

Rauhofer, J. 2008. Privacy is dead, get over it! Information privacy and the dream of a risk free society. *Information and Communications Technology Law* 17(3):185-197.

SAITNews. 2010. DA alleges eNatis corruption. http://www.saitnews.co.za/index.php?nav=articles&view=174 (Accessed 15 November 2010).

SANRAL. 2010. National Roads Agency. http://www.nra.co.za/live/index.php (Accessed 12 July 2010).

Shank, R. 1986. Privacy: history, legal, social, and ethical aspects. *Library Trends* 4:7-15.

South Africa. 1996. Constitution of the Republic of South Africa, No 108 of 1996. Pretoria: Government Printer.

South Africa. 2010. Protection of Information Bill, No 6 of 2010. Pretoria: Government Printer.

Stair, RM. 1992. Principles of information systems. A managerial approach. Boston, MA: Boyd & Fraser.

Wikipedia. 2010. Automatic number plate recognition. http://en.wikipedia.org/wiki/Automatic_number_plate_recognition#cite_note-16 (Accessed 14 August 2010).