Information Privacy Concerns in a Participatory Crowdsourcing Smart City Project

Liezel Cilliers, Stephen Flowerday
Department of Information Systems
University of Fort Hare

Abstract

'Smart Cities' are an innovative approach that allows for current city infrastructure and resources to be used more efficiently. Large amounts of data must be collected for a smart city to be effective, but there are information security concerns that prevent citizens from participating in these projects. This paper investigates what factors need to be in place in order to mitigate the information security concerns of citizens participating in a public safety, participatory crowdsourcing smart city project. The study made use of a quantitative approach with a survey design. A questionnaire was completed by 361 participants of a public safety project hosted East London, South Africa. The results indicated that information security was a concern to the participants. The factors that were identified to mitigate the information security concerns included: legislation; the continuous availability of the crowdsourcing system; education to increase awareness about the information security controls in place and feedback mechanisms to provide evidence about how the reported information is being used to increase public safety in the city.

1. Introduction

The population living in urban areas is increasing at a steady rate. In 2012, more than fifty percent of the world population resided in cities, and it is predicted that by 2028 more than 80% of the world's population will have moved to cities in search of better economic opportunities and social services [1]. This urbanization trend provides a variety of challenges to city management as three quarters of the world's natural resources are consumed in cities [2]. Typical challenges include the loss of basic functionalities such as waste management, air pollution, traffic congestion and health and safety in the city [1]. Furthermore, local authorities must provide services to the increasing urban population making use of deteriorating infrastructure, limited budgets and diminishing resources [3]. When governments find that they no longer keep up with the demand for service delivery, the only solution is to find alternative methods to use existing resources more effectively [4]. In order to do this, local authorities are employing Information and Communication Technology (ICT) to make their city 'smarter'.

The goals of a smart city are to improve the quality of life of the citizens and provide sustainable services [5]. Smart Cities makes use of ICT in order to integrate and connect services through the combined use of software systems, server and network infrastructure and client devices. The services that can be improved making use of smart cities include city administration, education, healthcare, public safety, real estate, transportation and utilities [4]. These services can benefit when making use of smart technology as the infrastructure and services become more efficient, resource friendly and safe, which allows for better management [6]. However, in order to accomplish these goals, large amounts of data must be collected that can be analyzed in order to anticipate upcoming events or to isolate problem areas [7].

The collection of unprecedented amounts of information from citizens may lead to privacy and information security concerns which can impede the adoption of smart city services [2, 5, 8]. Privacy concerns are especially prevalent when data is collected making use of crowdsensing [3]. 'Crowdsensing' is a term used to refer to the involuntary participation of the end-user who is making use of a mobile device with various sensors attached to it [9]. As this type of data gathering is involuntary, the participant does not have control over what, when or where the data is being recorded. Once citizens are aware that their private information will be collected, they are often not willing to participate in crowdsensing campaigns [10].

By contrast, participatory crowdsourcing is voluntary because individuals can choose what they want to report according to what they observe in their immediate environment [11]. The data that is gathered can then be analyzed in order to anticipate upcoming events or isolate problem areas [12]. Therefore, participatory crowdsourcing can be used to overcome privacy concerns as the citizen can control what information is reported, however, once the citizen has reported the information they have no control over what happens to it [1]. Information security controls must be in place to ensure that the information reported to the crowdsourcing system remains confidential, have integrity and is available to the correct stakeholders [13].

This paper sets out to investigate what information security factors need to be in place in order to safeguard the information that citizens report to a participatory crowdsourcing smart city system. As large amounts of data must be collected in order for the smart city to be effective, it is important that the

information security concerns of citizens be addressed in order to increase participation. The paper is structured as follows: The next section will provide a discussion about smart cities and the data collection methods employed in these cities. Then, the concept of information security is discussed with particular reference to smart cities, after which a brief overview is provided of the methodology used in this study. Next, the results are presented and discussed. Lastly, the factors to mitigate information security concerns of citizens in a smart city are presented.

2. Background

2.1. Smart City

A smart city can be defined as follows: "… a city may be called smart when investments in human and social capital and modern ICT fuel sustainable economic growth and a high quality of life, as well as wise management of natural resources, through participatory government" [14, p. 6]. There are a variety of areas in the city that can be improved by making use of the smart city concept. These include the economy, energy, e-governance, mobility, environment and quality of citizens' living [5].

One of the most important aspects of a smart city is that it provides the citizens a voice in the management and governance of the city. By allowing citizens to participate and become more active, it provides for more informed and educated citizens. Hence, citizens are vital to the success or failure of the smart city project [15]. Also, for a smart city to function effectively and efficiently, large amounts of data must be collected [7]. Data collection methods, such as crowdsourcing or crowdsensing, may be used to provide a low cost and scalable way to access data that may be otherwise difficult to obtain [5]. Crowdsourcing is particularly useful in public safety situations where data can be collected from the 'crowd' to help victims of natural disasters and coordinate rescue operations [16]. The collected data is analyzed making use of predictive analytics to provide information to prepare for an emergency situation, provide an appropriate response during the emergency and recovery services afterwards.

Data can also be collected in a smart city making use of either opportunistic or participatory mobile devices. Opportunistic, or crowdsensing systems, makes use of sensors that are located in citizens' mobile phones to capture data. The citizen does not have control over when the data is collected and may not even be aware that smart phones have applications that can record their location and movements without their knowledge [8]. Information gathered from citizens can include time and location stamps that may reveal the routine of the citizen. Sound samples can record private conversations while background noises can reveal the current location of the citizen. Pictures and videos can divulge the social circle or behavior of the citizen. Biometric data may be used to determine the current physiological state of the citizen. All of these data sources pose a serious threat to the privacy of the citizen. Once citizens are aware that their privacy may be invaded, they are often reluctant to participate in crowdsensing campaigns [10].

Participatory crowdsourcing, on the other hand, refers to the voluntary participation of individuals who are able to choose when and what they want to report [17]. This approach is particularly useful for unusual events such as accidents or other public safety related issues [8]. As the citizen is able to control the data that is reported to a participatory crowdsourcing system, privacy concerns are minimal.

In the public safety context, crowdsourcing serves a further purpose as the citizens can report unusual public safety events, such as motor vehicle accidents, in a wider geographical area making use of their mobile phone [10]. Participatory crowdsourcing has been used successfully in man-made and natural disasters to gather real-time information from the field and thus improve crisis management [16]. Examples of such projects include the Haiti earthquake in 2010, Hurricane Sandy in 2012, Uttarakhand Flood Crisis mapping in 2013 and Typhoon Haiyan in the Philippines in 2013. Citizens use the system to volunteer information; communicate with others to identify resources to common problems, or access advice from experts [16].

Before citizens will make use of any crowdsourcing system, they do consider the level of privacy, information security and anonymity that the system affords them [16]. The information that is reported to the crowdsourcing system can be used to identify the reporter, and therefore the information security controls of the system must be in place in order to protect the privacy of the citizen. Furthermore, information security and privacy threat has been identified as one of the most important considerations for citizens to decide if they are willing to participate in smart city initiatives [16]. The next section will discuss these two threats.

A. Informaton Security

The definition of privacy that is most apt for a smart city is that of Westin [18] that states: "the claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Making use of this definition, participatory crowdsourcing is the best way to protect the privacy of the citizen as they can control what information is reported and when. There are several vulnerable instances along the crowdsourcing process where information can be made available to unauthorized parties. These instances can be divided into three areas: when the information is being reported, processed and stored.

Participatory crowdsourcing initiatives to improve public safety in a city often make use of mobile phones due to their portability and ease of use. In developing countries, where technology infrastructure is not always available, the existing mobile infrastructure can be used to decrease the cost of a smart city project. Mobile penetration in South Africa is reported to be at 91% [19]. Illiterate users can also make use of a crowdsourcing system to report public safety information. Previous studies have reported that illiterate people can use a telephone keypad [15]. The high cost of telephone calls and data in South Africa can also discourage citizens to report public safety matters to the crowdsourcing system. This problem can be overcome by incorporating a mobi site or toll-

free number in the project making it more affordable for citizens to report public safety information. Furthermore, citizens that are not familiar with a crowdsourcing system can use the mobi site to report information at their own speed.

Mobile phones do expose citizens to new types of information security threats. Mobile devices are vulnerable to security breaches as the devices lack the computational speed and storage capacity of personal computers. This means that traditional cryptographic techniques cannot be used as protection measures. Mobile phones are also vulnerable to physical security threats e.g. if the phone is stolen or eavesdroppers [5, 8]. If a citizen's identity is revealed, they could become vulnerable to fraud, identify theft or online attacks such as spam or phishing [8].

Once the information has been reported using the crowdsourcing system, citizens have no control over what happens to the information. Citizens are often unaware how applications they download onto their phones will collect and use their personal information and the privacy risks associated with these processes. The developers of the mobile applications also neglect to inform citizens about the collection, processing and transmission of location-based data. This means that the user of the application is left to blindly trust the their private data is being stored and used properly and not directed to unauthorized destinations such as advertisers [8]. In a public safety situation, the citizen is required to provide a reasonable amount of information in order to enable emergency services to respond appropriately. The ability to combine citizens' self-reported data with other data sources poses a serious risk to the privacy of the citizen.

The combination of various data sources have the potential to yield new and sensitive insights beyond the comfort level of the citizens who are not aware of how their data will be used. Cellular phones have the capability to automatically capture user locations and movement from one destination to the next. Coupled with the large amount of data that is collected from the citizen, the smart phone can be used to 'watch' over the activities of the citizen. The ability of the smart phone can be viewed as an intrusion of user privacy and as a result, citizens might refrain from using smart city services to avert the Big Brother effect [5, 8]

3. Methodology

A positivistic, quantitative study design was used in this project. The study population identified for this research project was citizens living in East London, South Africa. East London has a current population of 440 000 [20]. Fifty-seven percent of the population is reported to be living below the poverty line while unemployment is reported at 28% [21]. The majority of the population lives on the periphery of the city where the infrastructure and services are poor and the unemployment rate is high.

In East London, the Directorate of Health and Public Safety are responsible for the public safety of citizens. The Directorate has three divisions: traffic and law enforcement, fire and rescue services, and disaster management [22]. However, the functions of these divisions are not integrated as they tend to function in silos.

The University of Fort Hare, in conjunction with IBM, developed an Interactive Voice Response (IVR) system and mobi site which allowed members of the public to report their public safety matters. An IVR system is suitable for developing countries as existing telephone infrastructure can be used; citizens unfamiliar with the technology can report public safety matters at their own pace while the IVR system would not exclude illiterate citizens from the project [19]. Residents were recruited through marketing in the local newspapers, distribution of flyers and social media to participate in the project.

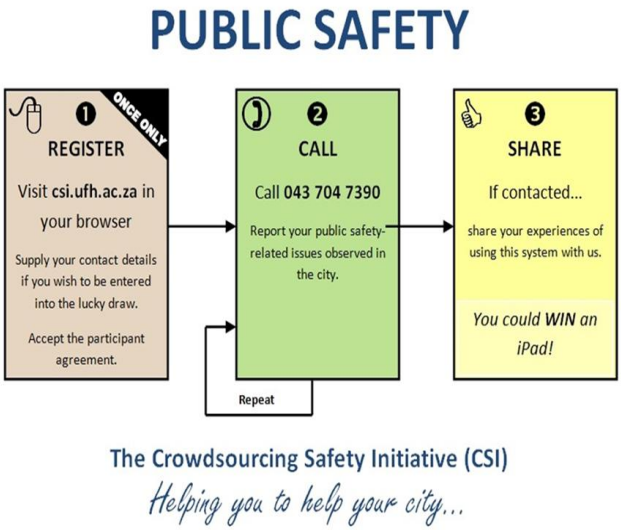

Figure 1. Steps in the Public Safety Project

Figure 1 is a graphical representation of the project. During the first step of the project participants registered on the official Public Safety Initiative website. Step two comprised calling the number provided and reporting a public safety matter. Step three entailed completing the online questionnaire that was sent to the registered participants in order to share their experiences of the system.

English was chosen as the primary language for the voice prompts so as to encourage the citizens to provide reports in the same language, because the use of English facilitated the analytics conducted on the reports. Accordingly, the participant used voice prompts to navigate the system and to report their information.

These voice prompts were structured as follows:

- Welcome message
- Did the participant consent to the terms and conditions of the study?
  - If "yes", continue
  - If "no", refer to website and call ended

- Participant is asked to record message that includes the relevant details:
  - Date, time, location, type of incident and details of incident
- If the participant is not satisfied with the recording, they are given a chance to record the message again.

Additional prompts and call flows were designed to accommodate situations where the user entered incorrect information or the user input was not recognized by the application. The application was tested rigorously by users working in the researchers' department.

In addition to the IVR system, citizens could also make use of mobi site to report their public safety matters. The high cost of telephone calls in South Africa, coupled with an unemployment rate, make a mobi site or toll-free number a suitable alternative to the IVR system. The citizens indicated during the survey that they did not have a preference between the mobi site and IVR system when reporting public safety matters. The reported data was used in predictive analysis in order to identify problem areas in East London where the limited public safety resources would have the biggest impact, if deployed.

A total of 485 people registered for the project, and after reporting a public safety matter, were sent a questionnaire to complete. The questionnaire sent to the study participants was compiled making use of previously published material in the information security field. A total of 361 questionnaires were completed. Thus, the response rate was 81.2%. The Cronbach's Alpha coefficient was conducted and was found to be 0.9. This is considered to indicate good test reliability. Ethical approval for the study was obtained from the Research Ethics Committee of the University of Fort Hare.

4. Results

The objective of this study was to investigate what factors need to be in place in order to mitigate the information security concerns of citizens making use of a public safety, participatory crowdsourcing smart city project. The study sample consisted of 219 (60.7%) males and 142 (39.3%) females. Seventy one percent of the participants were younger than 40 years of age. The 40−49 years age group consisted of 14.7% of the study sample, while the two oldest age groups, 50−59 and 60+, and were the smallest groups with percentages of 10.2% and 3.3%, respectively.

Table 1. Demographics of Participants

Gender	Males	60.7%
	Females	39.3%
Age Group	Less than 40 years	71%
	40-49 years	14.7%
	50-59 years	10.2%
	Older than 60 years	3.3%

One of the most commonly used frameworks in ICT security is the "C-I-A triad". The questionnaire tested three constructs in the information security field: Confidentiality, Integrity and Availability of the data. The 3 major objectives that must be considered when implementing a security framework in ICT include Confidentiality (preventing disclosure of communications between sender and receiver whether intentional or unintentional), Integrity (ensuring the accuracy and consistency of information as it moves through all parts of the network), and Availability (making sure that all who are authorized to access network resources are able to do so reliably and without undue delay) [19].

Table 2. Results of the Questionnaire

Category	Question	Mean	Agree	Disagree
Confidentiality	I prefer to provide information anonymously	2.1 (Agree)	72.6 %	5.6%
Integrity	I do not worry that the information I provided will be modified in any way	2.45 (Agree)	62.5 %	18.61%
Availability	The IVR system must be available 100% of the time in order to be useful	1.8 (Agree)	86.6 %	3.4%
Benevolence	If the information I reported is improperly disclosed to a third party, the impact for me could be potentially devastating	2.4 (Agree)	62%	19.2%

The first question related to the confidentiality of the citizen which is closely related to privacy [13]. The majority of participants (72.6%) indicated that they would prefer to report public safety information anonymously when making use of a participatory crowdsourcing system. Furthermore, the majority of the participants (62.0%) believed that if the information that was reported via the participatory crowdsourcing system were disclosed to a third party, this may have negative consequences for the person reporting the information,

Integrity refers to the safeguarding of the accuracy and completeness of information and its processing methods [13]. The results showed that 18.61% of the participants were concerned about who would have access to the public safety information reported via the crowdsourcing system.

The crowdsourcing system is intended for emergency and non-emergency reporting, thus it is essential that information reported be reliable and available when needed. The majority of the participants (86.6%) indicated that they believed that the information should be available 100% of the time in order to be useful.

The results of Table 2 show that the participants in the study were aware and concerned about the information security of the participatory crowdsourcing system. These results will be used to inform the recommendations to safeguard the information security of a public safety, participatory crowdsourcing system.

5. Discussion

Smart cities need to collect large amounts of information to function effectively. In order to promote the participation of citizens in a smart city project, the information security concerns of the citizen must be addressed [8]. Making use of literature and the results in the previous section, three categories of core factors were identified as crucial when making use of a public safety, participatory crowdsourcing system. These categories include the institution, technology and people of a smart city [2].

5.1. Institution of a smart city

The majority of the participants in the study preferred to remain anonymous when reporting to the participatory crowdsourcing system. Confidentiality is closely linked to privacy. The privacy concerns of the participants are clear as almost two thirds indicated that they would expect harmful consequences if the information reported to the participatory crowdsourcing system were to be made available to unauthorized parties.

There are four risks that will affect the privacy of citizens if the information reported to a participatory crowdsourcing system were to be made available to unauthorized people or used for malicious purposes [15]. The four risks include the intrusion upon one's private affairs, seclusion and solitude; disclosure of embarrassing private facts about the individual in public; defamation of character arising from having "private facts" misrepresented in public, and identity appropriation or theft for personal gain by others [18].

When making decisions about information systems that manage personal information, privacy legislation must be used as the appropriate guideline [13]. The standard, the ISO/IEC 29100: 2011, is an internationally accepted standard of good practice for information security and are widely used to inform information privacy policies in various contexts. The standard may be used by all types of organizations that deal with and depend on information, e.g. commercial enterprises of all sizes, charities and government. This, in turn, renders it suitable for a participatory crowdsourcing system in which both government and citizens will participate in information sharing as the standard is flexible enough to allow organizations to choose what controls to include according to the individual need [19]. The aim of the standard is to provide a set of suggested controls designed to address information security risks, including confidentiality, integrity and availability and are therefore appropriate to protect the privacy of citizens in a smart city project. The principles can be seen in Table 3 [13].

Legislation must be used to protect the privacy, and confidentiality, of citizens in a smart city. Furthermore, citizens must be educated about the collection, analysis and use of the information that they report to the participatory crowdsourcing system in order to promote transparency and trust [5]. The next section will discuss how the technology used in a smart city can mitigate the information security concerns of citizens.

TABLE 3. ISO/IEC 29100: 2011 [13]

ISO/IEC 29100 – Privacy Principles
1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

5.2. Technology of a smart city

Smart cities rely on both the quality and availability of the ICT infrastructure in a city [19]. In developing countries, problems such as the lack of ICT infrastructure and unreliable electricity supply often prevent new ICT investments.

However, as crowdsourcing makes use of the existing telephone infrastructure, the implementation costs of this technology is minimal [23].

If the crowdsourcing system is not available when needed, especially in the public safety context, it will not be considered dependable and will impact on the ability of the emergency services to provide an adequate response. This is seen in the response of the participants where the majority indicated that the system must be available 100% of the time to be useful.

In order to protect the integrity of the information, there are a number of technical solutions which are available to secure the information reported to a crowdsourcing system. These include encryption, digital signatures and server reliability [5].

In addition to the legislation that is used to ensure the confidentiality of the citizens, technology can also be used to protect the identity of the citizen. Statistical Disclosure Control (SDC) can be used in conjunction with techniques such as noise addition, micro-aggregation, rank swapping and rounding and pseudonyms [5]. SDC protects the privacy of the individual while allowing the release of their data for secondary use. The privacy of the individual is protected as the techniques mentioned above are used to distort the data in order to avoid linkages of the private information while protecting the data utility. The next section will discuss the third category, the people of a smart city.

5.3. People of a smart city

The citizen must trust that the necessary controls are in place in order to engage meaningfully with the participatory crowdsourcing system [24]. It is not reasonable to expect a system to be 100% secure as additional investments in controls or safeguards will not eliminate all risk entirely. However, the level of trust of the citizen will be affected by the perception of how adequate or inadequate the controls are that must protect their private information [13].

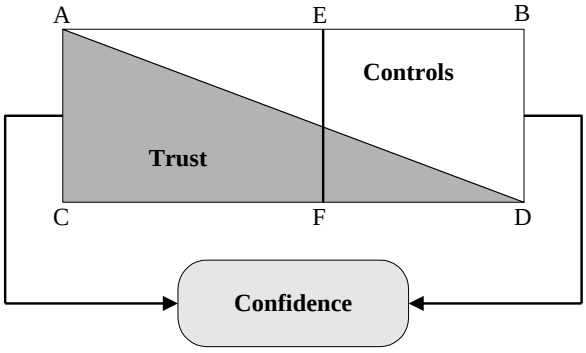

Figure 2. The Relationship Between Trust and Controls in a Crowdsourcing System [24]

Figure 2 illustrates how trust and controls work together to create the perception of security in a participatory crowdsourcing system. The rectangular area, A, B, D, C, represents the interaction between the citizen and participatory crowdsourcing system, while triangle A, B, D represents the controls that are inherent to the crowdsourcing system. Triangle A, D, C represents the trust that the citizen have in the system to protect their privacy. The line E-F is the hypothetical positioning of the citizen's Risk Appetite, the position of which can be influenced by the individual's propensity to accept risk. When considering the Risk Appetite line it is clear that the white area is protected by controls and the dark area, which presents risk, is protected by trust.

This means that the confidence of an individual can be influenced by both trust and controls, but that the extent of this confidence will depend on the Risk Appetite line of the individual. As line E-F moves further left, the system controls put in place decreases and subsequently the risk (and associated trust the individual has to display), increases [13].

The information security controls implemented in a crowdsourcing system is often not explained to the citizens, which means that they are expected to blindly trust that the data is properly secured and will not be made available to unauthorized parties [8]. The appropriateness and distribution of the information reported to a participatory crowdsourcing system will alleviate the information integrity and availability concerns of the citizens. Appropriateness determines whether the revelation of particular information would be appropriate in a given context, while distribution focuses on information transfer from one party to another. For example, the citizen reporting the data may not participate in a crowdsourcing project depending on the number of recipients that would have access to his/her data [10]. The local authority must make the process of data storage and analysis transparent in order to inform citizens how these concerns will be dealt with. For this reason, feedback mechanisms must be in place to provide the necessary proof to citizens that the information reported is properly secured. By increasing the awareness about information security controls of participatory crowdsourcing systems, the perceived risks associated with the system will also be decreased. This in turn will also alleviate fears from citizens that the information will be made available to unauthorized parties or modified [13].

The onus rests on the local authority, which is the information custodians, to communicate with the citizens how the information reported to the participatory crowdsourcing system will be used. The local authority was elected by the citizens to that position and, therefore it is incumbent on the local authority to act in the best interests of the citizens. Factors that influence the perceived benevolence of the local authority include the consistency of the party's actions in the past, credible communications about what was done with the reported information, and the extent to which the local authorities actions are congruent with his/her words [19]. Feedback mechanisms that illustrate to the citizens that the information reported are being used in a proactive way to

isolate or prevent problem areas will contribute to the increased participation of the citizens in a smart city project.

6. Conclusion

Local authorities must find ways to make use of existing resources more effectively and efficiently. Smart cities make use of ICT to collect data that can be analyzed to predict where resources will be needed or have the largest impact. In order to collect data, crowdsensing or crowdsourcing can be used. Crowdsensing poses serious privacy threats to the citizens participating in smart city projects, while participatory crowdsourcing largely circumvent the problem of privacy as the citizen can control what data is reported.

However, before citizens will make use of a participatory crowdsourcing system, they do consider the information security concerns associated with it. Information security concerns of a participatory crowdsourcing system include physical threats associated with mobile phones; lack of security controls where the data is stored and the purpose for which the data is collected. The confidentiality, availability and integrity of the data also must be considered.

In order to alleviate these fears, three factors were identified: legislation, technology and people of a smart city. Both legislation and technology can be used to protect the confidentiality and privacy of citizens, while the technology must always be available in order to be useful in a public safety situation. Education must be used to increase the awareness of citizens regarding the information security controls in place to protect the integrity of the information. In addition, feedback mechanisms are useful to provide evidence to the citizens about the purpose of the information that is being reported.

Further research in the field needs to investigate what are the privacy concerns of citizens in a crowdsensing system and what factors will alleviate these concerns. Appropriate feedback mechanisms must also be investigated to find the most appropriate mechanism for the public safety context.

7. Acknowledgment

This research project was funded in part by IBM and NRF.

8. References

[1] K. McConnachie, “Smart cities: Data analytics transform urban living,” Retrieved February 10, 2013, from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=59869, 2012.

[2] T. Nam and T.A. Pardo, “Smart City as Urban Innovation: Focusing on Management, Policy, and Context”, Proceedings of the ICEGOV2011, Estonia, p. 182-192, 2014.

[3] T. Nam, and T.A. Pardo, “Conceptualizing Smart City with Dimensions of Technology, People, and Institutions”, Proceedings of the 12th Annual International Conference on Digital Government Research, New York, p. 282-291, 2011.

[4] C. Harrison and IA. Donnelly, “A theory of smart cities”, Proceedings of the 55th Annual Meeting of the ISSS, 55(1), 2011.

[5] A. Martinez-Balleste, P.A. Perez-Martinez and A Solanas, “The Pursuit of Citizens’ Privacy: A Privacy-Aware Smart City is Possible”, IEEE Communications Magazine, p. 136-141, 2013.

[6] HU. Buhl and M. Jetter. “BISE’s responsibility for our planet”. Business & Information Systems Engineering, 1(4), 273–276, 2009.

[7] T. Dimitriou, “Smart Internet of things in future cities (with emphasis on security)”, Berlin: Germany, 2012.

[8] Y. Wang, Y. Huang and C. Louis, “Respecting User Privacy in Mobile Crowdsourcing”, Proceedings of the ASE2012, London, p1-15, 2012.

[9] M. Demirbas, MA. Bayir, CG. Akcora, YS. Yilmaz and H. Ferhatosmanoglu, “Crowd-sourced sensing and collaboration using Twitter”. In World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium, pp. 1–9, 2009.

[10] D. Christen, S. Kanhere, A. Reinhardt and M. Hollick, “A survey on privacy in mobile participatory sensing applications”, Journal of Systems and Software, 84(11), 1928–1946, 2011.

[11] B. Bhaveer, S. Flowerday and A. Satt, “Using Participatory Crowdsourcing in South Africa to Create a Safer Living Environment”, International Journal of Distributed Sensor Networks, 2013, p. 1-13, 2013.

[12] APA. Ling and M. Masao, “Smart Grid Information Security (IS) Functional Requirements”, arXiv preprint arXiv:1109.4474, 2011.

[13] L.D. Introna, “Privacy and the Computer: Why we need privacy in the Information Society”, Metaphilosophy , 28(3), p. 259-275, 1997.

[14] A. Caragliu, C. Del Bo and P. Nijkamp, “ Smart cities in Europe. Series research memoranda 0048”, Amsterdam: University of Amsterdam, 2009.

[15] H. Chourabi, T. Nam, S. Walker, J. Gil-Garcia, S. Mellouli and K Nahon, “Understanding smart cities: An integrative framework”, In Proceedings of the 45th System Science Hawaii International Conference , Hawaii, p. 2289–2297, 2012.

[16] B. Halder, “Evolution of Crowdsourcing: Potential data protection, privacy and security concerns under the new Media Age”, Democracia Digital e Governo Eletrônico, Florianópolis, p. 377-393, 2014.

[17] S.M. Mehta, "Mobile 311: A framework for 311 services with mobile technology", San Diego: San Diego State University, 2011.

[18] A.F. Westin, "Privacy and Freedom", New York: Atheneum Publishers, 1967.

[19] M. Whitman and H. Mattord, "Principles of information security", Boston: Thomson Course Technology, 2009.

[20] StatsSA, "Key results: Census 2011". Available at www.statssa.gov.za/Census2011/.../Census_2011_Key_results.pdf. (Accessed 02/05/2013), 2013

[21] S. Managa, "Unfulfilled promises and their consequences: A reflection on local government performance and the critical issue of poor service delivery in South Africa". Africa Institute of South Africa, 76, 1–8, 2012.

[22] Buffalo City Metro, The municipality: "How it works". Available at www.buffalocity.gov.za/municipality/ keydocs/idp2007/updated_analysis.pdf. (Accessed 10/05/2013), 2012.

[23] A. Kumar, S. Agarwal and P. Manwani, "The spoken web application framework: user generated content and service creation though low-end mobiles", In Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility, 2. New York: ACM, 2010.

[24] S. Flowerday & R. Von Solms, "Trust: An element of information security", In Security and Privacy in Dynamic Environments, pp. 87-98.

