**Privacy Issues in Smart City: Model, Threats and Solutions**

**Introduction**

Cities provide more jobs, higher salary and comfort place for modern society. But industrial city brings many city diseases such as pollution, traffic jam, high criminal rates and lack of green space to people’s life. Therefore, Smart city is created as a new concept to make city safe, sustainable, environmental friendly and interconnected by information and communication technology (Sen et al.,2013). By using these technologies, such as WIFI, QR code and other digital devices in citizens’ daily life, New York, Songdo and Shanghai make themselves full of competitiveness to attract well-educated people and investment (Angelidou, 2014; Guo et.al, 2016).

However, more information technology involves to people’s life, more negative privacy issues may make people frustrated and make their privacy more vulnerable. People may suffer hacking, identity theft and other privacy issues during smart city development. Smart devices and technology arise some threats which may damage people’s digital identity in their daily life (Baldini et al.,2013). In technology level, people do not have any privacy. But people still try their best to protect their privacy, because Internet and communication technology in smart city development would make cyber security gains more attention (Cerrudo, 2015). Thus, privacy issues become a vital problem for smart city development.

Most scholars focus on individual topics and concepts, and show less attention on how to combine these ideas together to build a complete structure to emphasize privacy issues in smart city: Angelidou (2014) and Guo et.al (2016) focused on smart city development. Sneps-Sneppe & Namiot (2016), Luvisi & Lorenzini (2014), Pan et.al (2013), Cerrudo (2015) and Elmaghraby & Losavio (2014) did research about technology and crime issues in smart city, which shows negative influence to people’s privacy. Martínez-Ballesté et.al (2013), Pérez-Martínez & Solanas (2011) and Domingo-Ferrer (2007) studied privacy issues in smart city and build three different privacy models. Sen & Nath (2013) and Baldini et.al (2013) tried to find solutions for privacy issues in smart city. Thus, making these concepts connect with each other become necessary for urban policy scholars. Furthermore, Scholars always try to solve privacy issues by technology and private section. They ignore public section which plays a significant role in smart city development.

To make different concept connect with each other. I reorganized these concepts to make them rational. So, in this paper, different paper may emphasize different sections and answer different questions. This paper tries to build a complete structure for privacy issues in smart city and identify what public section can do to help people protect their privacy by legislation, supervision and public management. Therefore, people can enhance their privacy awareness and policy makers can find some good suggestions for future smart city development to reduce privacy risks.

**Privacy Issues in Smart City: 3D Model, W³ Model and 5D Model**

Domingo-Ferrer (2007) identified that respondent privacy, user privacy and owner privacy are three kinds of database privacy. Respondent privacy tried to avoid re-identification which information is already in database. User privacy focus on protecting requirement made by users. Owner privacy is make sure who entitle which items. This model tries to identify people’s privacies during the using process. But it is too abstract to make people may not understand completely.

Pérez-Martínez and Solanas (2011) defined W³ privacy model which can be concluded in one sentence: Someone is asking for something near somewhere. The three W are where, what and who. “Where” focus on users’ geography position. If location privacy leaks, users would be tracked. “What” relates to user’s actions, which full of personal information. “Who” is users’ private identity which may bring opportunities to build users’ personal profile. W³ model bases on specific issues which easy for people to understand. But this model still to general, many privacies are still not identified, for example footprint privacy.

Martínez-Ballesté et.al (2013) combined 3D model with W³ model and created their own model which is 5D privacy model which includes identity privacy, query privacy, location privacy, footprint privacy and owner privacy. Identity privacy means when users disclose their identity to service provider, their privacy should be protected. Query privacy suggests that users’ requirement should be secured by service provider. Location privacy is users’ physical location information should be preserved. Footprint privacy is service provider should not leak any information which relates what users did in the past. Owner privacy means users maintain their own items and information which do not belong to service provider and other third parties.

Martínez-Ballesté et.al (2013) compared their own model with 3D and W³ model in the following table. It is easy to find that 5D model bases on 3D and W³ model. But they borrowed too much ideas from existing models and generated less new perspectives. For future research about privacy model, scholars should analyze using process and separate this process into more different sections to identify more different privacies.



**What Makes Privacy Vulnerable in Smart City?**

**Crime issues**

Sen & Nath (2013) thought hacking smart software can cause a system failure and malfunction, because smart software provides basic function for devices. If the software is the key of public management system, city would be completely go into a chaos. This is a general description about hacking threats. Some skilled attackers may set companies, city service systems and governments as their targets, these attackers are well organized and hard to defend by individual power (Cerrudo, 2015). Some powerful organizations cannot defend themselves perfectly, people’s privacy must more vulnerable.

**Cyber Privacy Awareness**

Cerrudo (2015) focued on cyber security problems which cause by less attention. He identifies some cities do not test cyber protections issues before they apply new technologies which may cause privacy risks. Because of software and systems are not perfect enough, some bugs still exist. By breaking these bugs, attackers can invade system easily. Sen & Nath (2013) also found some datasets are not authenticated, which may cause potential privacy risks. In smart city, all hosts are required to show their identity, and all datasets in smart city system should be valid. But government and citizens still need to develop their privacy awareness and make sure these datasets are valid and trusted when they access to smart city. Thus, enhancing privacy awareness in smart city can help people and organizations reduce privacy risks. Because more preparation must benefit future development.

**Technology**

Sen & Nath (2013) identified how smart software generate privacy risk when people access them. Because bugs and backdoors in software may cause personal profiles disclosure. Programmers should take responsibility to make their software stronger.

Sneps-Sneppe and Namiot (2016) looked at how mobile cloud computing works in smart city. They identify 4 different layer: data center, Infrastructure as a Service(IaaS), Platform as a Service(PasS) and Software as a Service(SaaS). In smart city, people update their information and documents to cloud and download them from cloud. How to make cloud safe become a significant issue for both people and companies. If cloud broke by attackers, all private information would lose, which must damage people’s privacy.

Pan et.al (2013) identified four kinds of data tracking sources which are mobile devices, vehicles, smart cards and floating sensors. They also found human behavior, social relation and city dynamic are significant areas which tracking technology focuses.

Tracking technology brings benefit to people’s life, they can track their order, bus and find more interesting articles to read. But tracking also damages people’s privacy. Because company know people’s interests and send some advertises to them. If criminal know some rich people’s location, a kidnap may happen. By tracking people’s relation, criminals may use people’s identity defraud their friends and family.

**Potential Solutions**

Elmaghraby and Losavio (2014) generated a model about cyber privacy security issues in smart city. When they identify solutions, they believe capable guardians who may not legal authorities but can help people recover their systems and repair errors. In smart city, programmer plays an important role in smart city development. Because software is the key component for smart city, people cannot live in a smart city without software. But most people do not comfortable to deal with software problem. So, programmer should take more responsibility to help people protect their privacy.

Baldini et. al (2013) created a Trusted Usage Framework to protect citizens’ life in some crisis cases without hurt their privacy. In their research, Trusted Usage Framework bases on digital identity, trust and usage control. Digital identity is a kind of proof to get access to devices. Trust is for some emergence case which asking information to identify who to do what at every time. This framework may work, but how to build trust still a huge problem for people.

Cerrudo (2015) did a research about how to avoid cyber-attacks and why people’s privacy become vulnerable which identified encryption could be one key issue for people to protect their privacy. Encryption brings directly help to people’s privacy, but people still need to pay more attention on password disclosure. Luvisi and Lorenzini (2014) claimed that RFID technology is a new system to make supply chains more efficiency by several electronic devices and label. QR code is one key aspect in RFID technology. By using QR code, people can access to smart city network more safe, more convenient and more directly.

Sen et.al (2013) thought authentication of datasets could be one significant aspect for government to focus. Government should take responsibility to verify these datasets, because only government has executive power to make these datasets legal and link to people’s life.

**Discussion: How to Solve Privacy Issues by Public Section**

Many papers try to solve smart city privacy problem by technology and social effort, while they ignore that public section can show a great influence to reduce privacy risks in smart city. Therefore, to identify what government can do, what legislature can do and what NGO can do to solve smart city privacy problem become an academic gap for future research. This pare would provide some general description about these topics.

In big government country, government can use most public management methods to protect people’s privacy, for example public firewall and encryption system. But for small government country, it should be in a different situation. These governments should pay less attention to public management, but need to focus on supervision to make sure internet companies walk in a right way.

Legislature should active a specific law about cyber privacy to bring the strongest shield for people to protect themselves. A specific commission also could be built by legislature to generate greater supervision to make sure companies can do their best to protect their customer’s privacy.

NGO is a special force for privacy issues in smart city. Because of they do not have any power, what they can do is finishing more research about privacy issues and help people defend their rights when they suffer some privacy problems. By focusing on society and people’s daily life, NGO’s work may enhance people’s privacy awareness and teach them how to protect their privacy by themselves.

**Conclusion**

This paper identified privacy issues in smart city by providing three different privacy models. Crime issues, cyber privacy awareness and technology are key aspects which may damage people’s privacy in smart city. To protect people’s privacy, social effort and technology support are necessary. Finally, this paper discusses about how to protect people’s privacy by public section, which includes government, legislatures and NGO. For future study, how to make government involve to privacy issues in smart city more comfortable becomes significant for scholars. Because many people think it is an offend if government involve their private life.

**Reference**

Angelidou, M. (2014). Smart city policies: A spatial approach. Cities, 41, S3-S11.

Baldini, G., Kounelis, I., Fovino, I. N., & Neisse, R. (2013, September). A framework for privacy protection and usage control of personal data in a smart city scenario. In International Workshop on Critical Information Infrastructures Security (pp. 212-217). Springer International Publishing.

Cerrudo, C. (2015). An emerging US (and world) threat: Cities wide open to cyber-attacks. Securing Smart Cities.

CITIES, S. (2013). Trace analysis and mining for smart cities: issues, methods, and applications. IEEE Communications Magazine, 121.

Domingo-Ferrer, J. (2007, September). A three-dimensional conceptual framework for database privacy. In Workshop on Secure Data Management (pp. 193-202). Springer Berlin Heidelberg.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4), 491-497.

Guo, M., Liu, Y., Yu, H., Hu, B., & Sang, Z. (2016). An overview of smart city in China. China

Luvisi, A., & Lorenzini, G. (2014). RFID-plants in the smart city: Applications and outlook for urban green management. Urban Forestry & Urban Greening, 13(4), 630-637.

Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Communications Magazine, 51(6), 136-141.

Pérez-Martínez, P. A., & Solanas, A. (2011). W3-privacy: the three dimensions of user privacy in LBS. In 12th ACM Int’l. Symp. Mobile Ad Hoc Networking and Computing.

Sneps-Sneppe, M., & Namiot, D. (2016). On Mobile Cloud for Smart City Applications. arXiv preprint

Sen, M., Dutt, A., Agarwal, S., & Nath, A. (2013, April). Issues of privacy and security in the role of software in smart cities. In Communication Systems and Network Technologies (CSNT), 2013 International Conference on (pp. 518-523). IEEE.