IADIS International Journal on WWW/Internet
Vol. 13, No. 1, pp. 1-16
ISSN: 1645-7641

DESIGN OF SMART CITY SYSTEMS FROM A PRIVACY PERSPECTIVE

Anna Ståhlbröst. *Luleå University of Technology*

Ali Padyab. *Luleå University of Technology*

Annika Sällström. *Agio Sofware*

Danilo Hollosi. *Fraunhofer Institute for Digital Media Technology*

ABSTRACT

All around the globe the concept of smart cities is growing at fast pace meaning that an increasingly amount of people are moving to cities, which causes problems for cities with energy supply, waste management, transportation, environmental issues and security to mention a few. To answer to these challenges, the concept of smart cities emerges referring to cities that invest in human and social capital, and traditional (transport) and modern (ICT) communication infrastructure that will fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance. Hence, for cities to be smart they cannot only install technologies, but they also need to invest in human capital and sustain a high quality of life. It is therefore important that solutions being implemented in smart cities answer to the needs and expectations citizens have as well as protect them from being exposed or forced into unwanted situations. In earlier studies it has become clear that people often are worried about their privacy due to our life being so easy to track and technologies becoming increasingly ubiquitous and pervasive. In this paper we will report on a study carried out with focus on understanding citizens view on information privacy concerns related to an intelligent acoustic smart city solution for audio monitoring. By means of this technology it was possible to detect events such as sirens, recognise speech commands and detects presence in public buildings. Audio monitoring is a relatively new and under research phenomena. Hence, in this paper an analysis of a survey on information privacy concerns, carried out with 1000 respondents around Europe, is presented and discussed. The basic findings from this study indicate that people have information privacy concerns related to this type of solution on a general level. However, when being more thoroughly introduced to the solution and its usage area, the citizens also became more positive towards the solution. The study also identified design principles that aims to support the design and implementation of smart city solutions that take not only users, but also affectees perspectives into consideration.

KEYWORDS

Smart cities, Citizens, Information Privacy, Audio Monitoring, Action Design Research, Design Principles

1. INTRODUCTION

All around the globe, cities and their surrounding regions, are growing at fast pace and it is claimed that over 50% of our global population now live in cities (e.g. Lee & Lee, 2014; Liu et al., 2014). This rapid growth causes possibilities and challenges for cities, which now are facing the challenge of simultaneously combining both competitiveness and sustainable urban development. and as such the challenges many cities need to encounter is to sustain their competitiveness, being environmentally sustainable, offering a high level of livability for its citizens, as well as supporting social inclusion and equity (Newton, 2012). Hence, cities are complex systems characterized by massive number of interconnected citizens, businesses, communication networks as well as services and utilities (Neirotti et al., 2014). Smart cities therefore, needs to combine and balance factors such as: economy, mobility, environment, people, living and governance, built on the smart combination of endowment and activities of self-decisive, independent and aware citizens.

There are many existing definitions of what a smart city is and in this paper, but for the purpose of this paper we align with the following definition stating that a city is considered to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance (Caragliu et al., 2011). Hence, smart city services are becoming a norm rather than an exception due to the rapid growth and utilization of ICT (Lee & Lee, 2014), and is further augmented by ubiquitous technology such as, e.g. internet of things and mobile computing. These technologies can be used to support, for instance constant monitoring of key-infrastructures, just-in-time maintenance, faster emergency responses, better and cheaper services for citizens just to name a few areas (Liu et al., 2014). But a smart city does not only entail technology changes but also investments in human capital and an alteration of urban living practices and conditions (Neirotti et al., 2014). Hence a smart city offers many possibilities and challenges related to both social and technological perspectives.

Due to the ubiquity and pervasiveness of smart city solution it is not always apparent for citizens where smart city solutions are installed, what type of data that is collected, stored and managed, or even for what purpose data is gathered for, and about, the citizens and the city. Due to the huge impact of the digitalization, usage of ICT is visible in almost all facets of citizen's life and this gives a vast amount of data about a person. Living in the digitalized and smart society implies that we, to some extent, give up some details in our private lives, leading to an increased risk of loss of privacy. This can make citizens more vulnerable and thus, the importance of protecting their privacy becomes increasingly important (e.g. Bélanger & Crossler, 2011; Hough, 2009). It is therefore important to understand how to design innovative ICT-solutions for smart cities that do not invade citizen's privacy.

The increase of digitalized information, i.e. big data, and advances of ICT put forward new information privacy challenges for multiple stakeholders such as business leaders, privacy activities, scholars and individuals (Smith et al., 2011). However, studying and understanding

how people's privacy is affected by the use of ICT in different contexts is a complex task since privacy can mean different things to different people. But even though this is the case, it is important to understand people´s perception of privacy in relation to smart city ICT solutions. As stated by Hong & Thong (2013), information privacy is one of the most important issues to handle in the information age due to the increased use of personalized and digitalized information. Often, invasion of peoples privacy are not intentional but due to designers incapability to foresee how the collected data could be used and how this might impact the users (Karat et al., 2005). This calls for a need of more research on how privacy can be considered in design processes (Little et al., 2005), i.e. privacy by design to ensure that users privacy is protected and considered early on in the design. Embedding privacy preserving mechanisms into the design will ensure that the new technology will be adopted by the citizens while minimizing the barriers to the wide acceptance of the technology (Miorandi et al., 2012). In a smart city context, citizens communicate with a large number of different ICT devices which are prone to different breaches of personal information or a so called "Big Brother" effect. Since real smart cities count on their citizens, they need to abide and fulfill their privacy needs (Martinez-Balleste et al., 2013).

The aim of this research was to gain understanding of citizen's perspective on privacy issues related to a smart city solution being implemented both outdoor in the streets as well as in public buildings. Due to the approach of our research, being inspired by action design research, the results from the studies also influenced the design of the system. Based on the results from our studies, design principles for smart city systems have been developed.

In this paper we will report on the EU-FP7 project EAR-IT (ID 318381) in which the objective was to develop and test intelligent acoustic technologies in a city context with the goal to contribute to the development of smart city solutions. Developing smart city solutions is a multi-stakeholder challenge, but here, the focus is on one aspect, namely the citizens since designing a solution for a smart city context includes considering the citizens who might be exposed to this type of technology. Therefore, one part of the EAR-IT project was to consider privacy aspects and include these in the design of the final system by applying a privacy by design approach. In previous research on information privacy (e.g. Bélanger & Crossler, 2011; Hong & Thong, 2013; Pavlou, 2011; Smith et al., 2011), audio monitoring, or intelligent acoustics, seems to be an area that has not caught a lot of attention among privacy researchers. Hence, in this paper, we will contribute to that area by analysing and discussing a smart city solution for audio monitoring from an information privacy perspective and based on that suggest design principles to support the design of future smart city solutions.

The remainder of the paper is designed as follows. Firstly we will give an introduction to the field of information privacy that is followed by a description of our case, EAR-IT. Thereafter, our action design research methodology is described and discussed followed by an illustration of our results. Finally, lessons learned from this study flowed by practical implications and design principles for smart city solutions are presented.

2. INFORMATION PRIVACY

Privacy is often thought of as a human right that can be seen from both a moral and legal perspective, and it is often viewed as the right to be left alone. In this paper we focus in particular on personal information privacy. This category of privacy can be defined as one´s

ability to control when, how and to what extent personal information is collected (Westin, 1968). Personal information is any information related to an individual identified directly or indirectly by that information.

In previous research regarding information privacy, six key dimensions that are most commonly utilized in prior conceptualization of information (and internet) privacy concerns has been identified (Hong & Thong, 2013; Malhotra et al., 2007; Smith et al., 1996; Smith et al., 2011; Son & Kim, 2008). These key dimensions are:

- Collection; refers to the situation that large amounts of personal and identifiable data on individuals are gathered, and refers to the degree to which a person is concerned about the amount of individual specific data possessed (Malhotra et al. 2004)
- Secondary usage: means that personal information is collected for one purpose, but is used for another without proper authorization from the individual (Junglas et al., 2008)
- Errors: is the degree to which a person is concerned that protections against deliberate and accidental errors in personal data collected are inadequate
- Improper access: refers to the degree to which a person is concerned that personal information is readily available to people not properly authorized to view or work with the data (Smith et al., 2011)
- Control: relates to a persons concern that s/he do not have adequate control over his/her personal information (Malhotra, 2004)
- Awareness: is the degree to which a person is concerned about his/her awareness of information privacy practices (Malhotra, 2004)

Often when information privacy is studied the focus is to understand an individual's perception of his or her concern for how personal information is collected and handled by a website for, e.g. shopping (Bélanger & Crossler, 2011; Clarke, 1999; Hong & Thong, 2013; Junglas et al., 2008; Smith et al., 1996). Weinberg et al. (2015) argue that privacy is the most prominent issue within application of IoT that is distinguished from Web 2.0 and creates new challenges to share and expose more information and keeping fewer secrets. Hence, the scope of many previous studies is slightly different than ours that focus on privacy issues related to a smart city solution for audio monitoring supported by internet-based technologies where citizens are largely unaware of the fact that data is being collected in their context. The resemblance between our study and previous studies is that the technology developed in this project facilitates collection, storage and processing of data supported by internet technology and it is an organization behind the collection. Thus, the frameworks used in previous information privacy studies (e.g. Clarke, 1999; Hong & Thong, 2013; Price et al., 2005; Son & Kim, 2008) have been modified and applied in our study.

Since Smart City solutions often are both ubiquitous and pervasive we have also looked into privacy design principles suggested within that area of research. There have been attempts to propose privacy by design principles in the sub-context of smart cities like smart grids (e.g. Cavoukian et al., 2010) or IoT (e.g. Babar et al., 2010). In 2001, Langheinrich contributed to the area of privacy by design by developing practices that supports the development of privacy enhanced UbiComp systems (Langheinrich, 2001)ngheinrich, 2001). These practices are described as:

- Notice: If personal data is being collected from a user, they should always be aware of it.
- Choice and consent: The user should have the choice of sharing, or not, of their personal data. They should give their explicit consent.
- Proximity and locality: The collection of data from a user's device should only occur when the user is present (proximity). Processing and access to these data should only be done within the space they were collected (locality).
- Anonymity and pseudonymity: Whenever the user's identity is not required or whenever the user does not consent, anonymity or pseudonymity services should be provided for.
- Security: There should be security mechanisms, which provide adequate protection for collected data.
- Access and resource: Access to the user's data should only be allowed to authorized persons. There should be regulatory means for the protection of a user against parties that are not complying with this regulatory framework.

As the development of technologies today moves into the direction of becoming increasingly invisible, smart and mobile, also other aspects of information privacy become important to consider since improper handling of such information can expose private persons to significant risks (Hough, 2009).

Based on the dimensions and practices presented above we can see that these are not really related to smart city solutions, or solutions that are implemented in a context where people are affected by the technology, but not being users of it. One might argue that these type of systems do not collect personal data and thus do not have to oblige to the same rules and laws that systems that collect personal data does. However, we argue that due to technologies becoming increasingly sophisticated and pervasive, new types of privacy issues emerge which has to be taken into considerations when smart city solutions are designed and implemented.

Personal privacy expectations are affected by the introduction of new technologies (Friedewald et al., 2007), and intelligent acoustics is one of the new research streams which research for privacy requirements is demanding.

3. ACTION DESIGN RESEARCH AND THE EAR-IT CASE

This paper is explorative and focus on understanding citizen's perspective on privacy issues related to a smart city solution. Hence, we explore a smart city innovation process with citizen engagement, and we do that based on a EU funded project called EAR-IT. In this research project, the overarching research and design methodology was influenced by action design research (ADR) (Sein et al., 2011). This research methods are typically applied in project focusing on generating design knowledge through the building and evaluating of IT artifacts (Sein et al., 2011). Following the recommendations by Maccani, Donnellan & Helfert (2014) ADR is a suitable methodology for conducting research in smart city contexts. This approach deals with two challenges, firstly the methodology addresses a problem situation encountered in a specific setting by intervening and evaluating, and secondly, constructing and evaluating an IT artefact that addresses the identified class of problem. In general, ADR consists of four main phases (Sein et al., 2011). The first is the problem formulation, focusing on identifying

and conceptualizing a research problem which in our case was to understand how to design a smart city solution based on Internet of Things without endangering peoples personal privacy. In this phase we also created a long-term commitment by constructing a project including dedicated partners, and dividing roles and responsibilities. The second phase in ADR is focused on building, intervention and evaluation (Sein et al., 2011). In this phase there was an intervention between city stakeholders, the building of the artifact and evaluating the artifact both on an early design stage as well as in its real world city context. Hence, this stage was carried out in two iterations. The third phase, is reflection and learning in which the learning is moved from the solution to applying learning to a broader class of problems (Sein et al., 2011). In our case this was made by relating our learning from citizen engagement to the problem of designing smart city sensing solutions that protect people's privacy. The final phase of action design research is formalizing learning. In this phase the researcher presents the accomplishments instantiated in the system and define the results, for instance as design principles (Maccani et al., 2014; Sein et al., 2011). In the end of the paper we will present the design principles that constitute our formalized learning based on this project.

3.1 The EAR-IT Case

In this paper, we use the EAR-IT project in which we wanted to gain understanding of citizen's perspectives on smart city installations in their context. This project started with formulating the research problem, then we interacted with contributors, citizens, and city stakeholders, through series of iterative phases of investigating, designing, intervening and finally evaluating the artefact in the city context.

This EAR-IT case, was an EU FP7 funded project, starting in 2012 and ending in 2014, which focused on large scale "real-life" experimentations of intelligent acoustics for smart cities. This project had the objective to develop high societal value applications and deliver new innovative range of services and applications mainly targeting smart-buildings and smart-cities. The technology being developed was early stage innovation hence the project was focused on experimentation and piloting, not develop a solution to be fully implemented at large scale.

The technology being developed in this project was intelligent acoustic solution providing "situational awareness" by using audio monitoring in combination with Internet of Things (IoT) technologies. This was achieved via a deployment of Audio Processing Units (APUs) in the targeted in-door and out-door environments as complementary to intelligent sensors already available in two test-beds (HOBNET, ID 257466; Santander, ID 257992). The solution was developed through collaboration between researchers and city stakeholders, including citizens. The APU consisted of a microphone and an embedded processing platform that continuously "listened" to its environment and analysed the sound locally. The technology was implemented and tested outdoor in a city context and indoor in public buildings such as a university and an office.

After identifying the problem and solution space, the artefact was designed to set up the technology and to make sure that algorithm e.g. event triggers, were fully functioning. Thereafter, the first interaction with citizens was carried out and the results from this interaction led to an identification of design principles and thus a redesign of the solution to make sure that no human voice was stored and transmitted, and that human voice could not be detected. The involvement of citizens was designed as a three-stage process that started with a

structured survey on information privacy in general to a broad population consisting of 1000 citizens in five countries. The second stage was to investigate the affectees attitudes towards this type of technology in the implementation stage and the third stage was to explore the affectees' experiences of being exposed to the technology over time. The evaluation of the IT artefact was performed in a real world context since the system was tested both in the city context in the streets as well as in public buildings.

In this paper we will report on the results from the first stage of the study. This first stage focused on gaining insights into citizens' attitudes perception of their information privacy related to audio monitoring in public spaces focusing on audio and acoustics. The result of this survey was used as input to guide the further development and implementation of the technology in the citizens´ contexts both outdoor and indoor, taking privacy issues into account to ensure that their privacy remain intact.

To support our research, we used the established framework for information privacy concerns developed by Smith, Milberg, Burke (1996) and being further developed several other researchers (Hong & Thong, 2013; Junglas et al., 2008; Son & Kim, 2008; Xu, 2007) as a basis for our questionnaire. In this framework, the question items have been tested and validated and it is established within the information privacy research community. In our study, we have deliberately, pointed the questions towards the citizens audio to get their opinion of "a worst case scenario" from which we then design the future technical solution by incorporating privacy by design aspects from the very beginning.

The questionnaire was divided into two sections, firstly the outdoor usage situation and secondly, the indoor usage situation. In each section, questions of general character were asked followed by some possible usage scenarios of the collected data to which the users responded. In this section of the questionnaire, each question was formulated as a proposition formulated as "I would be concerned if…" Related to each proposition, the citizens responded on a seven graded Likert scale from "I do not agree at all" (1), to, "I totally agree" (7). The propositions were divided into five themes, collection, secondary use, improper access, control and awareness. Finally, some general questions were asked.

The survey was distributed in five different countries, Sweden, France, Spain, Germany and Portugal. The questionnaire was carried out in April 2013 and 1000 citizens were contacted and answered the questionnaire in the five different countries involving 200 citizens each. Among these citizens the gender distribution was 50/50. The age distribution was almost evenly distributed, except for the ages between 61-69 years, which are under-represented with only 9% of the respondents.

4. RESULTS FROM DATA COLLECTION

In this section, we will present the findings from the survey divided in eight main topics including familiarity with audio-monitoring, data collection and use in relation to privacy, privacy perspectives of different usage-scenarios and open aspects and risks.

4.1 Familiarity with the Concept of Audio Monitoring

To start with, we wanted to gain insights into the citizens and their familiarity with the concept of audio monitoring since the concept as such is not widely distributed and

implemented. This revealed that 65,2 % were not at all familiar with audio monitoring. Looking into the different ages we saw that people in the age of 18-30 years old were the group where most stated that they were familiar with the concept with 27.4% being familiar to it. In the group 51-60, 17.4% stated that they were not at all familiar with the concept of audio monitoring. This shows that audio monitoring is a concept not so widely known.

4.2 Collection of Personal Data

Thereafter we asked about collection of personal data. Here, the respondents stated that they have concerns when their audio is being collected. Based on their results we can see that the main concern for citizens related to this issue, was that the organisations could collect more information than they need for their purposes. We also asked the respondents about their thoughts of a city collecting audio in public spaces around the city. Related to that issues, 6.8% of the respondents stated that they were not at all concerned about audio being collected from them, while 32.7% stated that they were concerned (7 on the scale). Here most of the respondents (n618) stated that they agreed to some extent that they would be concerned (5-7 on the scale). Based on this result it can be concluded that the respondents have concerns about their audio being collected, both from a general perspective and if audio is collected in public spaces.

4.3 Secondary use of Data and Improper Access

The next step of our survey was to investigate the respondents concerns about secondary use of their data, see table 1 below. This refers to the degree to which a person is concerned that their personal information is collected for one purpose but is used for another, which can be understood as secondary use without authorization from the individual (Hong & Thong, 2013). In our study we found that all the respondents raise concerns that the data being collected from them could be used for other purposes than what was initially agreed upon and aimed for. Most of the respondents show some concerns about their personal information being used for other purposes than stated (71% answered 5-7 on the scale). Here we also saw that 71.6% of the respondents was concerned about the data being sold to other organizations than had collected it in the first place. In addition, 71.1% agreed that they were concerned that their data could be shared with other organizations without their authorization. In relation to secondary usage and improper access, the respondents main concern was the organization collecting the data would share the data with other organizations

When it comes to the protection of their data from unauthorized access, 16% of the respondents did not agree that this was a concern for them (1-3 on the scale), while 65.7 % answered on the scale 5-7 that they agreed they were concerned about this. 18.3% were neutral answering 4 on the Likert scale. The respondents also agreed that they had some concerns related to if the organization collecting the data also would devote enough efforts to protect their data. Here 67.7% agreed that they had some concerns ranging from 5-7 on the scale, where 37% answered 7. In sum, the answers show that the respondents were concerned about their data being used for other purposes than initially stated, and we can also see that they have concerns about how the organisation the data will handle the data. Will they sell it, share it with other organisations than was firstly agreed upon and will they actually be able to protect the data for a longer period of time was issues citizens were concerned about.

Table 1. Improper Access

Improper Access Descriptive Statistics				
	Minimum	Maximum	Mean	Std. Deviation
I am concerned that the organisation collecting the audio is not protected from unauthorized access	1 = 6.4% 2 = 4% 3 = 5.6% 4 = 18.3%	5 = 13.9% 6 = 14.2% 7 = 37.6%	5.22	1.841
I am concerned that the organisation collecting the audio does not devote enough time and effort to prevent unauthorized access to the data	1 = 6.1% 2 = 4.8% 3 = 5.1% 4 = 16.3%	5 = 15.1% 6 = 15.6 % 7 = 37%	5.24	1.832

4.4 Control and Awareness

Another factor we looked into in our study was the respondents concerns about control and awareness of their audio being collected. This factor reflects the degree to which a person is concerned that s/he has control over the personal data held by the organization (Hong & Thong, 2013). Losing control over their personal data was also an issue that most of respondents agreed to have some concerns about. Here, the concern with the highest ranking was their concern that they would not have control over how their personal data was collected and used by the collecting organization.

When it comes to awareness it is clear that the citizens are afraid that they will not know that their data is collected and they will not know for what purpose the data is collected and used or by whom.

4.5 Responses related to the Usage-Scenarios

In the questionnaire we also presented two different usage scenarios were we put the technology into an outdoor context and an indoor context. In relation to each context, a few scenarios describing the usage of the audio monitoring system were presented to the citizens for them to respond to. The first scenario described was audio being collected to detect events such as sirens with the purpose of controlling traffic lights to ease the way for, e.g. an ambulance. Related to the outdoor scenarios, most respondents (59.6%) agreed that they would feel comfortable, on the scale from 5-7, that their audio is collected for the purpose of detecting outstanding distinctive events.

Table 2. Event detection, out-door scenario

I would feel comfortable that my audio is collected with the aim to detect sirens or other outstanding distinctive events in an outdoor environment.		Frequency
Valid	I do not agree at all	87
	2	66
	3	53
	4	198
	5	185
	6	171
	I totally agree	240
	Total	1000

The second outdoor usage scenario that we presented to the citizens was audio that was collected in a cross road with the aim to estimate the current traffic density in a specific area. Related to this scenario, 51.6 % of the respondents stated that they were comfortable, between 5-7 on the scale, that their audio was collected for that purpose, while 20.5% were neutral and answered 4 on the scale. Related to that scenario, 25% was not positive and did not feel comfortable with audio being collected. In the third outdoor usage scenario the audio was collected with the purpose of detecting outstanding events such as a person screaming for help in a certain context. Here, 65.1 % of the respondents stated to be comfortable with this usage situation. These results show that the respondents are more comfortable with the technology when they see a benefit related to their safety.

Thereafter we presented the indoor usage scenarios. The first usage scenario we presented was audio-collection with the aim to detect presence in a building which then could control lightning, heating and air-condition with the objective to save energy. When it comes to the indoor usage scenarios, the citizens are to some extent positive towards audio. The second usage scenario was speech recognition which could control, for instance, curtains and lightning in a building. Here 52.4% would, (to different degrees) feel comfortable with the audio being monitored to detect presence in a building and 48.6 % answered that they would feel comfortable (5-7 on the scale) with a solution based on speech command recognition.

Table 3. Presence detection – Indoor scenario

I would feel comfortable that my audio is collected with the aim to detect presence in a building. If no presence is detected for a specified period of time, lightning, heating and air-conditioning can be switched off with the objective to save energy		Frequency
	I do not agree at all	109
	2	80
	3	94
	4	193
	5	161
	6	139
	I totally agree	224
	Total	1000

4.6 Functionalities in the System

In the questionnaire, we also asked a few questions about the citizens reaction and opinions related to how important, or relevant, some designed functionalities in the system were, see table 4. Related to this question, it can be concluded that the most important part for people is to be duly informed about the audio monitoring - with a mean score value at 5.91 on a 7 graded scale. It is also very important that a remote person cannot listen to the audio and that no audio is stored. The functionality the citizens were most worried about was the storage of the audio. Also storing the audio in combination with other data sources such as positioning or video got a high mean score value (4.85).

The questionnaire also included some open questions where citizens were asked to give their free thoughts about whether they perceived any privacy risks with audio monitoring. Related to that issue 54.7 % of the respondents answered that they did, 23.4% did not and 21.9% did not know.

Table 4. Functionalities of the system

	The audio is not combined with positioning	The audio is not combined with video	The audio is not stored	People are duly informed about the audio monitoring	No human speech can be listened to by a remote person	No person can be identified	No human voice is stored
N Valid	1000	1000	1000	1000	1000	1000	1000
Mean	4.85	4.99	5.44	5.91	5.79	5.36	5.33
Std. Deviation	1.824	1.838	1.702	1.545	1.638	1.808	1.762

5. DESIGNING WITH PRIVACY IN SMART CITY CONTEXTS

Based on our research there are number of contributions that can be made both to theory and practice. Starting with privacy related to smart city solutions we have identified individual's privacy concerns related to that field, which is an underexplored area in privacy research. The results of our study show that respondents are afraid that their privacy might be lost if pervasive smart city solutions such as audio monitoring is implemented in their context. The citizens have expressed a concern that their data might be collected for one purpose but will be used for another in the long run. This privacy concern can be understood viewed in the light of reserve as it is expressed by e.g. Pedersen (1999). The data being collected could contain personal aspects, which, in turn, could be revealed to others if the technology is used for other purposes than it has been designed for. Reserve relies on collection, dissemination and control of privacy, which also includes an aspect where people need to have control over their personal information in order to feel that they have reserve.

Our study also shows that audio monitoring includes concerns related to anonymity. This means that the citizens do not want to be identifiable by others (Pedersen, 1999) and they cannot use pseudonymity as suggested by (Langheinrich, 2001) since there is no system where the citizens enter their profile, they are rather just being exposed to it. In this study this is observed in, for example, their expressed desire that the audio could not be listened to by other persons, or that no human voice would be stored. In relation to that, the fear of potential abuse if the data material falls into the wrong hands becomes apparent. Our study shows the importance to differentiate between concerns of how the data is managed and used, and the management of the monitoring and collection of the data. This correlates with Hong and Thong (2013) who suggests that information privacy concerns should be divided into interaction management and information management dimensions when it comes to how personal information is managed. Our study shows that also these aspects are relevant when it comes to audio monitoring technologies. For example, concerns have been raised of loosing control over what happens with the collected data, which can be related to information management. Another perspective raised by the respondents and which can be related to information management in this study is the risk that the data starts being collected with an initial good purpose, but as time passes and circumstances change, for instance governments, management, ownership of technologies and data, the data that was collected might fall into the wrong hands and thus being used in an unintended manner.

Relating audio monitoring and privacy to the aspects of notice (Langheinrich, 2001) it is always, to some extent, easy to implement the technology illegally in a smart city context. Here, it might be useful to have some type of alert system that make citizens passing by aware that audio is being monitored in this area. Thus, citizens can have the power to choose another street or building to visit. Associated to the issue of notice is also the dimension of choice and consent (Langheinrich, 2001). Our study shows that one important concern among citizens is their awareness of data being collected at all. This is not only relevant for audio monitoring, but for all types of smart city solutions where data is collected without citizens being aware or informed about it. The fear as such can be explained by the type of privacy that is labelled solitude, which is the freedom from observation by others (Pedersen, 1999). Here, citizens need to feel that they are not being observed by their city government or others, without them knowing of it and explicitly giving their approval of it. In addition when people make conversations in public spaces, for instance in a café or while walking in the streets, these are sometimes experienced as both safer and more confidential than those held in private. This has to do with the fact that there are a lot of people around, and thus, the conversation is made private by being lost in the noise around them. Based on our interactions with the citizens we have found that in general they expect that others are not observing them or listening to them in public spaces. However, there is a great risk that collecting data in public spaces can invade citizen's privacy if they are not aware of the data being collected and the technology is sophisticated and powerful enough to identify single persons in a crowd. Giving consent and having a choice when it comes to smart city installations is not always easy. There is no button where the user can give their informed consent that their audio can be collected. And even if there was a button where they gave their consent, what choice did they actually have if they really need to walk in the particular street where the audio is, or visit the building?

Finally, this study helps to clarify the role of security and safety related to privacy issues. In this study, we found that this type of smart city solution, the acoustic sensing technology, has the potential to strengthen security and safety for citizens, which is viewed as a potential application area for the technology. As the usage of audio monitoring was explained in a

specific scenario focusing on safety the respondents had less concerns about their privacy. This is an interesting finding in relation to the privacy paradox (Smith et al., 2011) since people state that privacy is important for them, but at the same time they can be willing to sacrifice some parts of their privacy to feel more safe. Based on that, it is important for designers of smart city solutions to consider how to keep citizens privacy intact without forcing citizens to make compromises about their privacy in relation to safety and security.

5.1 Practical Implications to Privacy by Design Principles

Based on this study we can conclude that the citizens are not overly positive towards audio monitoring, hence, the design of this type of solutions needs to be handled with great care to succeed. This has at least two implications for the future design of audio monitoring solutions and smart city solutions in general. One is the information to the people being exposed to the technology, and the second are the functionalities of the final solution where privacy protection needs to be designed into the final smart city solution.

From an informative perspective, people must be duly informed about how the technology is functioning (at a level they understand) and how the data that is collected will be used. They also must be informed about what type of data that is being collected, how much data that is collected and for which purpose it is collected. How this should be accomplished in a smart city context includes many challenges since, for instance, signs explaining all this might not be an effective way to communicate as people do not always read signs, and informative meetings with citizens are usually only visited by a handful citizens. Hence, designing useful and communicate strategies for informing citizens are needed. Hence, some type of alert system needs to be implemented.

Sensor technologies such as audio monitoring are also powerful tools and it is therefore important to consider the potential maximum power of the technology when it is developed and implemented. Based on the results from this study we have developed a few design principles for how this type of smart city solutions can be designed to ensure that citizen's privacy are protected and considered when setting up smart city sensor networks. Even though the audio sensors did not store human voice or aimed at tracking individuals, it is important to keep in mind that it is not impossible to detect the persona behind a voice if the technology is sophisticated enough. It is not as easy to disguise your real-world appearance and voice as your online avatar or network cards. Hence, not storing audio, but data related to outstanding events, noise levels or direction of sound (not audio) is a more appropriate smart city solution.

Design Principles for Privacy Protective Smart City Systems	
Design principle	Description
General placement of sensors	Put sensors in a context where only general data can be collected that do not reveal personal information
No personal data storage	No storage of data that can be traced back to an individual (even if it is not personal data per se), it can be voice data or other data such as movement patters
Stream data	Stream data through the system instead of storing everything and make triggers recognise the data that are valuable for the system, focus on for instance outstanding events
Sensor systems in solitude	The system should not be combined with other technologies. Combining different data or systems could reveal a great amount of information about a person, which leads to increased risks of privacy invasion even though personal information is not collected individually in any of the system.

5.2 Limitations

In this study some aspects related to the approach of the study needs to be discussed and highlighted. The study showed that the respondents became more positive towards the technology and its usage as they saw the potential use of the technology in different scenarios. This calls for a more real-world oriented study focusing on the individuals experiences when people are exposed to the technology and the thoughts that emerge in that type of situation. We have done that during the project, but we have not reported on those results here, what we could see was that people in the outdoor scenario became more positive towards the system when they saw it in its context and was exposed to it. However, the people in the in-door scenario was more sceptical when they where exposed to the system in their real-world context. We have also seen tendencies in our material that the citizens are naïve to some extent when it comes to monitoring and sensing in public spaces. One common expression is that they have nothing to hide, and thus monitoring is considered positive if it increases their safety.

To criticise our own study we want to highlight the complexity of studying the concept privacy concerns. A person's attitude towards privacy concerns is influenced by many aspects, which have not been investigated in our study. For instance their previous privacy experiences, regulations, trust, and privacy awareness can influence their attitudes towards privacy concerns (Smith et al., 2011). If these aspects would have been included in this study, the results of the respondents privacy concerns might have shown a more diversified picture. In addition, the questions asked in the study might encourage negative answers. For instance the question "I am concerned that when my audio is collected, the organisation collecting the audio could use it for other reasons than stated". To this question the respondents were asked to grade their answer on a graded scale from I totally agree to I disagree totally. Here it is hard to see that any person would not have been concerned if an organisation collecting the audio could use it for other reasons than stated. To increase the validity and generalizability from our study we will continue looking into the framework and the wording of the questions in future studies.

ACKNOWLEDGEMENT

This work was funded by the European Commission under grant no. 318381 EAR-IT – Experimenting Acoustics in Real environments using Innovative Test-beds. The projects My Privacy Flag and IoT Lab, also sponsored by the European Commission, has also contributed to make this research possible.

REFERENCES

Babar, S., Mahalle, P., Stango, A., Prasad, N. and Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (Iot). In *Recent Trends in Network Security and Applications*. Berlin Heidelberg: Springer

Bélanger, F. and Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, Vol. 35, No. 4, pp.1017-1041.

Caragliu, A., Del Bo, C. and Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, Vol. 18, No. 2, pp.65-82.

Cavoukian, A., Polonetsky, J. and Wolf, C. (2010). Smartprivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. *Identity in the Information Society*, Vol. 3, No. 2, pp.275-294.

Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communication of the ACM*, Vol. 42, No. 2, pp.60-67.

EAR-IT. (ID 318381). Eu Fp7 Project Ear-It Experimenting Acoustics in Real Environment Using Innovative Test-Beds. (Id 318381). Online: Http://Www.Ear-It.Eu.

Friedewald, M., Vildjiounaite, E., Punie, Y. and Wright, D. (2007). Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis. *Telematics and Informatics*, Vol. 24, No. 1, pp.15-29.

HOBNET. (ID 257466). Eu Fp7 Hobnet Holistic Platform Design for Smart Buildings of the Future Internnet (Id257466).

Hong, W. and Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, Vol. 37, No. 1, pp.275-298.

Hough, M. (2009). Keeping It to Ourselves: Technology, Privacy, and the Loss of Reserve. *Technology in Society*, Vol. 31, No., pp.406-413.

Junglas, I., Johnson, N. and Spitzmüller, C. (2008). Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services. *European Journal of Information Systems*, Vol. 17, No. 387-402.

Karat, C.-M., Karat, J. and Brodie, C. (2005). Why Hci Research in Privacy and Security Is Critical Now. *International Journal of Human-Computer Studies*, Vol. 63, No. 1–2, pp.1-4.

Langheinrich, M., (2001). *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. In proceedings of Ubicomp 2001: Ubiquitous Computing, 1265,

Lee, J. and Lee, H. (2014). Developing and Validating a Citizen-Centric Typology for Smart City Services. *Government Information Quarterly*, Vol. 31, No. 1, pp.S93-S105.

Little, L., Briggs, P. and Coventry, L. (2005). Public Space Systems: Designing for Privacy? *International Journal of Human-Computer Studies*, Vol. 63, No. 1–2, pp.254-268.

Liu, Y., Wei, J. and Rodriguez, A. F. C. (2014). Development of a Strategic Value Assessment Model for Smart City. *International Journal of Mobile Communications*, Vol. 12, No. 4, pp.346-359.

Maccani, G., Donnellan, B. and Helfert, M. (2014). Action Design Research in Practice: The Case of Smart Cities. In *Advancing the Impact of Design Science: Moving from Theory to Practice*, edited by Tremblay, M.VanderMeer, D.Rothenberger, M.Gupta, A. and Yoon, V.: Springer International Publishing.

Malhotra, A., Gosain, S. and El Sawy, O. A. (2007). Leveraging Standard Electronic Business Interfaces to Enable Adaptive Supply Chain Partnerships. *INFORMATION SYSTEMS RESEARCH*, Vol. 18, No. 3, pp.260-279.

Martinez-Balleste, A., Perez-martinez, P. and Solanas, A. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *Communications Magazine, IEEE*, Vol. 51, No. 6, pp.136-141.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. . *Ad Hoc Networks*, Vol. 10, No. 7, pp.1497-1516.

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G. and Scorrano, F. (2014). Current Trends in Smart City Initiatives: Some Stylised Facts. *Cities*, Vol. 38, No., pp.25-36.

Newton, P. W. (2012). Liveable and Sustainable? Socio-Technical Challenges for Twenty-First-Century Cities. *Journal of Urban Technology*, Vol. 19, No. 1, pp.81-102.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, Vol. 35, No. 4, pp.977-988.

Pedersen, D. M. (1999). Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology*, Vol. 19, No. 4, pp.397-405.

Price, B. A., Adam, K. and Nuseibeh, B. (2005). Keeping Ubiquitous Computing to Yourself: A Practical Model for User Control of Privacy. *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp.228-253.

Santander, S. (ID 257992). Eu Fp7 Project Smart Santander (Id 257992).

Sein, M., K, Henfridsson, O., Purao, S., Rossi, M. and Lindgren, R. (2011). Action Design Research. *MIS Quarterly*, Vol. 35, No. 1, pp.37-56.

Smith, J., Milberg, S. and Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, Vol. 20, No. 2, pp.167-196.

Smith, J. H., Dinev, T. and Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, Vol. 35, No. 4, pp.989-1015.

Son, J.-Y. and Kim, S., S. (2008). Internet Users' Information and Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, Vol. 32, No. 3, pp.503-529.

Westin, A. F. (1968). Privacy and Freedom. *Washington and Lee Law Review*, Vol. 25, No. 1, pp.166.

Xu, H., (2007). *The Effects of Self-Construal and Percieved Control on Privacy Concerns*. In proceedings of 28th International Conference on Information Systems, Montreal, Canada, 1050,