The Privacy Paradox of Utilizing the Internet of Things and Wi-Fi Tracking in Smart Cities

Krystan ten Berg, Ton Spil, Robin Effing

The Privacy Paradox of utilizing the Internet of Things and Wi-Fi tracking in Smart Cities

Krystan ten Berg, Ton AM Spil & Robin Effing, University of Twente, krystan.tenberg@gmail.com, a.a.m.spil@utwente.nl, r.effing@utwente.nl

ABSTRACT – *In recent years, we have seen the increase of Internet of Things (IoT) solutions, products and services. The Internet of Things will capture a large amount of data pertaining from the environment, as well as their users. The real value of collecting data will be the result of data processing and aggregation in a large-scale where new knowledge can be extracted. However, such procedures can also lead to user privacy issues. This study describes what citizens do and do not know about Wi-Fi tracking and how that knowledge affects their responses to privacy and security risks. The results of this study showed that there is a lack of awareness towards Wi-Fi tracking by people in the municipality studied. The results show that most respondents are willing to cooperate with Wi-Fi tracking, despite the fact that most people have concerns of losing control about how their data is gathered and used. This study also found that respondents indicated Wi-Fi tracking as useful and especially safety is appointed as an important benefit of Wi-Fi tracking. The results of this study confirm that privacy, trust and perceived benefits significantly influence the willingness to disclose personal information.*

Key terms: Internet of things, privacy, adoption of IT

I. INTRODUCTION

Control of privacy is of increasing importance (Belanger & Crossler, 2011), especially in cases of smart cities. The Privacy Calculus Theory implies that, people decide both consciously and unconsciously about the privacy they are giving up, and the benefits they receive in return (Dinev & Hart, 2006). Most of the previous studies involving the privacy calculus, focused on e-commerce or services like Facebook and the behavior of the users towards data disclosure. In this study the focus lies on the privacy calculus and Wi-Fi tracking.

Earlier research, which has tried to understand consumers' attitudes towards this specific form of data collection, is often directed at student populations and on one level. This study is both important for investigating citizens attitudes towards being tracked, and for understanding how these attitudes relate to actual behavior. Van Slyke (et al., 2006) introduced the concept of trust into the privacy discussion and this study includes that discussion.

First, the method is described followed by a structured literature review and the results of the survey are given in chapter four. Chapter five analyses these results followed by conclusions.

II. BACKGROUND

The first part of the approach for this study is based on an in-depth grounded literature review of relevant studies as well as official documents of international institutions. The literature study is conducted with data bases such as Scopus, Sciencedirect, Web of science and Jstor. Keywords used to find articles related to the topic are, privacy calculus, Wi-Fi tracking, Privacy, sensing, internet of things (IOT), MAC address and Smart cities. Founded articles provide information about the concepts of smart cities, IOT and Wi-Fi tracking. For the chapters of this study, different search combinations are used. The combination “IOT AND Smart city” was used to find articles about the general description of these concepts and the link between them. From the large number of articles, the ones with the most citations where used. For the literature about Wi-Fi tracking, the key words “Mac address” AND “tracking” are used. This provided 68 results of which the most useable where selected. Furthermore, the search on the keyword phrase “privacy calculus“ provided us with 324 articles. The articles with the most citations where used to describe the model of the privacy calculus used in this article. By using the key words “privacy calculus and disclosure behavior” together, 1 of 9 articles was useable for this literature review. Furthermore, the keywords “Privacy AND tracking AND Smart city” provided 19 articles, from which this research used 2 to describe privacy concerns in smart cities. “privacy concerns AND data disclosure” provide articles also usable for the chapters about privacy concerns. Some of the most cited articles where used.

SMART CITIES, IOT AND WI-FI TRACKING

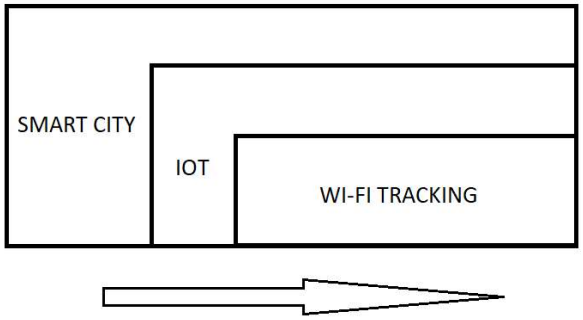
The Internet of Things (IoT) and Smart Cities are recent phenomena that have attracted the attention from both academia and industry. However Smart cities and The internet of things have different origins, they are moving towards each other to achieve a common goal (Perera, Zaslavsky, Christen & Georgakopoulos, 2014). In the following chapter,

the definition of a smart city will be described, followed by relevant points and problems in the context of the Internet of Things.

According to Hall, Bowerman, Braverman, Taylor, Todosow and Von Wimmersperg (2000), a smart city is a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens".
For a smart city initiative to be successful, urban development ICT and IOT are important building blocks in creating a smart infrastructure for managing ever increasing city population. The internet of things is one of the building blocks of a smart city. Sensing as a service model, as a solution based on IoT infrastructure has the capability to address the challenges in Smart Cities (Hollands, 2008). Smart Cities will take advantage of communication and sensor capabilities integrated into the cities' infrastructures to optimize electrical, transport, and other logistical operations supporting daily life, thereby improving the quality of life for everyone (Bartoli, Hernández-Serrano, Soriano, Dohler, Kountouris & Barthel 2011). In this respect, the IoT can become the building block to realize an unified urban scale ICT platform, thus unleashing the potential of the Smart City vision (Hernández-Muñoz, Vercher, Muñoz, Galache, Presser, Hernández Gómez & Pettersson, 2011; Mulligan & Olsson, 2013; Al-Dhubhani., Mehmood, Katib, & Algarni, 2017). So urban IoTs are designed to support the Smart City vision, because it aims at exploiting the most advanced communication technologies to support added-value services for the administration of the city and for the citizens (Zanella et al,. 2014).

Because Infrastructures are a central component of the Smart City and that technology is the enabler that makes it possible, but it is the combination, connection and integration of all systems what becomes fundamental for a city being truly smart (Nam and Pardo, 2011). The overall vision of the smart city needs IOT to unleash the potential of this vision. Figure 1 shows how the core components are related in this research. Smart city as an overall vision, IOT as building block to support the smart vision and Wi-Fi tracking as an application from this vision and technology. However, it must be noted that the direction of the relationship between these building blocks can be interpreted differently.

Fig.1



The real innovation in smart cities, comes from the Internet of Things, the ever-expanding network of sensors and devices that collect data everywhere. Atzori et al., 2010, stated that people might experience a real difficulty in understanding what IoT really means, which basic ideas stand behind this concept, and which social, economic and technical implications the full deployment of IoT will have. The Internet of Things represent an explosion of information creation, sharing, and use. This is due to greatly increased types and numbers of connected physical devices such as sensors and actuators, and systems used by people. Miorandi, Sicari, De Pellegrini, and Chlamtac(2012) stated that, the Internet of Things vision can provide a large set of opportunities to users, manufacturers and companies, including, e.g., environmental monitoring, health-care, inventory and product management, workplace and home support, security and surveillance. Because location information is a large component of IoT information, and concerns about its privacy are critical to widespread adoption and confidence, location privacy issues must be effectively addressed. (Minch, 2015). The Internet of Things is vulnerable to privacy violations. Previous research highlighted the fact that privacy could be a significant barrier to the growth of IoT (Perera et al.. 2015). As more connected objects become integrated in daily lives, ensuring that people feel comfortable with IoT's impact on their privacy becomes increasingly important.

PRIVACY IN THE INTERNET OF THINGS PARADOX

Privacy preservation will be one of the major challenges in the development of the Internet of Things. Billions of sensor-enabled devices will be deployed for collecting fine-grained information from the environment and will share them with other devices and backend servers (Lopez, Rios, Bao & Wang, 2017).

Monitoring and privacy

During the past decade, user privacy has become an important issue in networked computing environments. (Lee and Kobsa, 2016). The possibilities of data-gathering innovations that can underpin the smart-city framework is broad: street lights fitted with license plate readers, sensors that detect and count passing smart-phones, the presence of closed-circuit cameras in many cities etc. Many smart city technologies capture personally identifiable information (PII) and household level data about citizens – their characteristics, their location and movements, and their activities. As cities are becoming smart, people start to be increasingly aware about their surroundings, feeling more secure, but at the same time being more concerned about their privacy (Longo and Cheng 2015). Personal data is easily collected and analyzed through the use of sophisticated means of the smart-city. Mobile applications and devices are increasingly asking users to provide personal information, as well as monitoring users through behavioral tracking. Companies deploy several mesh of nodes in different area: individuals could be tracked in a large scale. Risks are higher if those localizations are correlated with other information (Demir, 2013). Collected data may than be capable of linking to or identifying an individual, which raises privacy concerns (Wilson and Valecich, 2012). This privacy-invasive practice is likely to increase with the proliferation of sensor devices in the upcoming era of Internet of Things. (Lee and Kobsa, 2017). In fact IoT and Ubiquitous technology are leading to increasing privacy as they are capturing and storing more and more information about people and their activities (Longo and Cheng, 2015).

Many definitions of privacy exist in literature. Privacy is inherently difficult to reduce to a single definition that is rich enough to explain perceptions and behaviors across a range of contexts (Vasalou, Joinson & Houghton 2015). Traditionally, privacy has been conceptualized as a right to control over information about oneself (Derikx, de Reuver, Kroesen and Bouwman (2015). Westin (1967) defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (as cited by Könings, Schaub, & Weber 2016). In general terms, privacy debates acceptable practices with regards to accessing and disclosing personal and sensitive information about a person (Elwood and Leszczynski (2011).

Within this research context, privacy is mostly related to location and movement and citizens ability to control their location relevant information. According to Finn, Wright and Friedewald, (2013) privacy of location and space implies that, individuals have the right to move about in public or semi-public space without being identified, tracked or monitored. They furthermore state that, such a conception of privacy has social value. When citizens are free to move about public space without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom.

Wi-Fi tracking and privacy

In the case of monitoring and Wi-Fi tracking, location and movement privacy are most likely to be violated. Privacy of location and space is especially impacted by tracking technologies in mobile phones, cars (Derikx et al., 2015) and location based services (Krumm, 2009). With the use of location based services, one of the biggest concerns is that it can be possible to compile a very detailed picture of someone's movements if they are carrying a wireless device that communicates its location to network operators. The potential for abuse of this information ranges from unsolicited advertisement from shops when a mobile user approaches, to the more serious concerns as, firms using location information on field employees to impose strict performance measures, and even dangerous or repressive, like criminals determining the right time to intrude on a subscriber's house, or an improper conviction made based on circumstantial location information (Beinat, 2001; Clarke, 2001) as cited by Steinfeld, (2004). However, the relative success of some location-based applications implies that at least some people are comfortable with sending their location data to third parties (Krumm, 2009).

Awareness

Demir (2013) concluded that people who are being surrounded by sensors embedded in their physical environment and capable of recognizing and responding to people's presence in a seamless and often invisible way, in which they are not aware of such collection, not knowing which information about them is collected, how it is being used, or with whom it may be shared down the road, will create privacy issues. Such a lack of transparency may undermine the ability of the user to effectively anticipate privacy risks associated with the collection and processing of his or her data, and subsequently take adequate countermeasures. As solution they propose to improved awareness & transparency of data practices. Users should be informed about when and how data is gathered, what kind of data is gathered, what is happening to this data and whether data might be shared with third parties. Most people are unaware that their Wi-Fi is a potential source of tracking (Demir, 2013). Public Wi-Fi is incredibly convenient, but raises privacy issues for users and potential backlash for Wi-Fi providers. Wi-Fi providers gathering mobile location data, consumers are being

tracked, often without they knowing it. Users' personal information is collected more passively and collectively. Users may feel less aware and in control of personal information being collected. According to Bailey, (2015), are consumers willing to trade off their privacy. And one possible reason as to why consumers are willing to trade away their privacy is because they are unaware of the amount of privacy that is being lost. He furthermore stated that, even if consumers were made aware of the loss, they would still engage in privacy-sacrificing behaviors. Behavioral economists have proven that people will both underestimate their risk of harm and prefer a short-term gain to a long-term risk. However, other studies found that, users often refuse to share their personal data with respect to time and space (Barkhuus and Dey, 2003).

The privacy paradox.

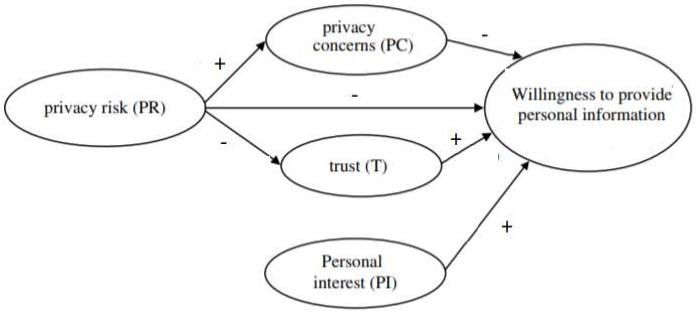


Fig. 2 Privacy calculus (Dinev and Hart 2006)

The discrepancy between actual or intended privacy related behavior and stated privacy is coined as the privacy paradox. Wilson and Valecich (2012) stated that the privacy calculus is a possible explanation for the privacy paradox. The privacy paradox is known as the discrepancy between the expressed concern and the actual behavior of users. In other words, people claim to be very worried about their privacy but do very little to protect their personal data (Barth and de Jong, 2017). The calculus perspective of information privacy interprets the individual's privacy interests as an exchange where individuals disclose their personal information in return for certain benefits (Xu,Teo, Tan & Agarwal, 2009).This is consistent with the study of Dinev and Hart (2006), they addresses the trade-off between the expected costs of privacy risk beliefs and the benefits of confidence and placement beliefs on the willingness to provide personal information. According to Dinev and Hart (2006), The perceived privacy risks reduce disclosure intentions while perceived benefits of information disclosure increase intentions. An individual's unique level of general privacy will increase their context-specific perceived risk and decrease disclosure intentions. Quite often the perceived benefits outweigh the perceived risks, which eventually leads to the neglecting of privacy concerns that often results in the disclosure of information in exchange for social or economic benefit (Privacy Calculus Theory; Culnan and Armstrong, 1999). Users consciously weigh the disadvantages of privacy disclosure against the perceived benefits. It would seem that users consciously resolve discrepancies between the willingness to obtain and possess something (such as downloading an app) and the simultaneous difficulties that arise in terms of unknown threats or risks (such as potential data usage by third parties (Barth & de Jong, 2017).

Constructs of the privacy calculus

The privacy calculus model (Figure 2) as proposed by Dinev and Hart (2006) is used in this research. The model of Dinev and hart exist of the following constructs; Risks, privacy concerns, Trust, Personal interest (benefits), and the willingness to provide personal information (in the rest of this study revered to as Attitude). The study of Barth and de Jong (2017) described the same constructs and added some more like; Awareness.

1. Privacy risks

Risk beliefs in this context, is defined as the expected loss potential associated with releasing personal information to a specific firm (Malhotra, Kim and Agarawal (2004); Lee & Rao, (2007). It also leads to fears of the actual uses of the obtained personal data. Prior privacy literature has identified sources of organizational opportunistic behavior, including unauthorized access and selling personal data to or sharing information with third parties, financial institutions, or government agencies (as cited by Xu et al., 2009). Improper handling of personal information could result in the discovery and matching of location data and identity (Clarke, 2001).

2. Privacy concerns

Malhotra et al. (2004) stated in their study that users privacy concerns are determined by three factors: Concerns about the collection of data, the control they perceive to have over this collection, and how important they consider being aware of data collection. Furthermore, the study of Smith, Milberg and Burke (1996), identified four dimensions of an individual's concern about privacy, namely: Collection, Errors, Unauthorized secondary use and Improper access (as cited by Liu, Shan, Bonazzi, R. and Pigneur, 2014). The four factors provide a framework to explain the concerns for information privacy (Stewart & Segars, 2002). That is, the likelihood of privacy breaches is expected to occur, when any of the following cases happens: (1) large amounts of personally identifiable data are being collected, (2) data are inaccurate, (3) companies use personal information for undisclosed purposes, and (4) companies fail to protect consumers' personal information (Liu et al,. 2014). Furthermore the study of Fogel & Nehmad (2009) found that, general privacy concerns and identity information disclosure-concerns are of greater concern to women than men.

3.Trust

In the case of trust, firms which implement fair information practices, and disclose these practices to their "customers" can exercise latitude in how they use personal information gathered, without risking customer defections and the other negative outcomes, they ensure that their practices are consistent with what they disclosed to their customers (Culnan & Armstrong, 1999). Institutional trust refers to an individual confidence that the data – requesting stakeholders or medium will not misuse his or her data (Anderson and Aqarwal 2011; Bansal et al 2010; Dinev and hart 2006 and had been found to be related to privacy concerns, risk beliefs (Malhotra et al 2004) and intentions to disclose information (Dinev and hart 2006).

Whereas trust may not necessarily eliminate risk beliefs, Dinev and Hart (2006) argue that it can overrule their negative impact (as stated by Krasnova, Veltri and Gunther, 2012). The cumulative effects of trust and personal interests can outweigh privacy risk perception to point that it eventually leads to the disclosure of personal information (Dinev and hart, 2006).

4.Personal interests (benefits)

Previous research about privacy from Van Zoonen (2016); Barkhuus and Dey, (2003); Wirz, Roggen & Troster, (2010) suggest that, people assess for which purpose data is used and weigh the benefits that providing their data may offer them. When these benefits are of immediate personal relevance (medical services, commercial gain), most people are willing to share their data with the organization asking for them (e.g. Acquisti, John, & Loewenstein, 2013). Heek, Arning and Ziefle, (2014) stated in their study for example that, surveillance technologies are accepted in those locations in which crime threat is present. Users then prefer safety over privacy. User diversity is a crucial factor in this context: Women attach a higher importance to safety in general, in contrast to men, while men prefer the protection of their privacy (Heek, Arning and Ziefle, 2014).

5.Attitude

The normalization of the collection and aggregation of data by governments raises also issues of privacy. Technologies and applications that were perceived to be creepy, have now become socially "acceptable" (Finch & Tene 2013). However, as stated before, privacy can be considered as a tradeoff between the disclosure of personal information and service related benefits (Chorppath & Alpcan, 2013; Dinev & Hart, 2006; Hann et al., 2007; Laudon, 1996; Li et al., 2010; Weinberg et al., 2015). On the one hand, people become increasingly critical of the protection of their personal data, such as online or offline tracking. On the other hand, are people willing to provide a lot of privacy if there is anything about it, for example free access to a Wi-Fi network. People care about privacy, but they may care even more about convenience. People have sacrificed their privacy over the last decades, and are probably continue to do so.

This paper will provide an answer for the following research question: *To what extent are citizens of the municipality aware that they can be tracked and how can the elements of risk, concerns, trust and benefits - as used in the privacy calculus - affect their attitude to data disclosure.*

IV. RESULTS

Data Collection – Questionnaire

The second part of the study consisted of a quantitative study for better understanding citizens' views on the topic. The data required to answer the main question is collected from a survey. In this section, will be discussed how the online survey data is collected and analyzed, and what can be learned about people's privacy preferences in IOT environments. The survey was administered to broad samples of individuals from the city studied, who were asked to participate voluntarily. The time period that this survey had been administered, is between January 2018 and March 2018. The target population for this study was inhabitants of a smart-city which is utilizing Wi-Fi tracking technologies.

To ensure construct validity, scales from previous studies will be adapted wherever possible. The survey included elements taken from the privacy calculus of Dinev and hart (2006) and Barth and de Jong (2017). The actual items were slightly adjusted from the original instruments to fit the city and Wi-Fi context of this study. Perceived risks and

benefits will be adapted from Xu et al. (2009) and general privacy concerns from Malhotra et al. (2004). The concept of trust was adapted from Dinev & Hart (2004, 2006), Malhotra et al. (2004) and Westin (2001), attitudes to disclose was assessed using scales adapted from Anderson and Agarwal (2011). On top of that, demographic variables such as age and gender were included. To prevent bias towards a negative or a positive attitude, the survey questions were formulated both positive and negative, depending on the construct. The outcomes of the survey were analyzed by using the software SPSS. Measure validation for reliability was established through examining Cronbach's alpha coefficient for each construct. Relations between the different constructs were analyzed with correlation and regression analysis. Because of the relatively limited set of respondents for the analysis, a 90% confidence interval was chosen.

The total amount of respondents is 86. All responses were valid with no missing answers. The distribution of male and female respondents was N= 51 and N=35. The Mean age was 34.56 (SD = 11.74) as shown in table 1. For the analysis the difference between male and female and age groups are taken in to account. For the most constructs no differences were found, however for the constructs awareness and privacy differences where noted.

		Frequency	Percent
Valid	Male	51	59,3
	Female	35	40,7
	Total	86	100,0

	N	Minimum	Maximum	Mean	Std. Deviation
AGE	86	21	63	34,58	11,730
Valid N (listwise)	86				

Table 1 - demographics

The descriptive analysis shows differences in the percentage the overall knowledge of Wi-Fi tracking and Wi-Fi tracking in Enschede. Almost 25% of the respondents had not heard of Wi-Fi tracking before. And more than 45% of the respondents were not aware of the fact, that Enschede also makes use of Wi-Fi tracking. There is however a difference between the age groups <42 and >43. The elderly group respondents (>43) are more aware of the fact that, the municipality of Enschede is using Wi-Fi tracking sensors in the city to track visitors (66,7%). From the younger group only 45,9 % of the respondents was aware of Wi-Fi tracking in Enschede.

Furthermore, 61,6% of the respondents indicated that they are not aware for what purposes municipalities are deploying Wi-Fi tracking sensors in cities. And more than 82% of the respondents are not aware that it is also possible that they can being tracked, without being connected to an open Wi-Fi network. What furthermore is striking is the fact that respondents of >43 are more aware of the fact that municipalities can track visitors in the city (84%) And in this age group 40 % is aware of the purposes of Wi-Fi tracking. More than 54% of the respondents thinks that Wi-Fi tracking can be useful. But they also believe that the interest of the citizens are always more important that the interest of municipalities 55%.

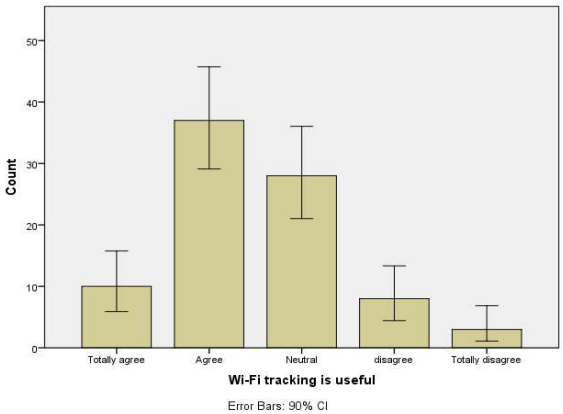
Most respondents don't know if they will experience (some) the benefits of a better city or services, when municipalities are gathering their data with Wi-Fi tracking. But most of the respondents think that Wi-Fi tracking is useful (54,7%).
Almost all respondents have chosen safety in cities as a possible benefit of Wi-Fi tracking (86%). Furthermore, better facilities in the city are also seen as a possible benefit by57%. Only n=6 (7%) of the respondents thinks Wi-Fi tracking cannot provide any benefit for them at all (table 3)

Frequencies

		Responses N	Percent of Cases
Benefits Wifi tracking[a]	Safety	74	86,0%
	Never	6	7,0%
	Offers	10	11,6%
	Facilities	49	57,0%
	Mapping	34	39,5%

a. Dichotomy group tabulated at value 1.

Table. 3 – main benefits and usefulness



In general the respondents do trust municipalities and government to handle personal data with confidence. There is no exception between the younger group of respondents (<42 and the older group (>43). However there is a difference between males and females. Males tend to have higher trust in how municipalities handle their data and existing laws and regulation than females do.

Most respondents are indicating that the gathering of personal data comprises risks. And most respondents stated that they worry about the gathering and handling of their personal data. Possible misuse of personal data is the biggest concern of respondents (60%). The results showed that the mean scores of the privacy are higher for females than for men, indicating that the group of females tend to have more concerns regarding their privacy.

Like the concerns, more than 51 % see the misuse of personal data as a (very) high risk. Actually, all the elements of risk are considered (very) high risks by respondents. Furthermore, most respondents (56%) worry that they will lose control about how their data is gathered and used. In the open comment section respondents indicated, that the possibility of their data being hacked is also a big risk.
Almost 40 % of the respondents indicated that they have no or less problems with Wi-Fi tracking, when they exactly know how there data is gathered and how it will be used. Only N=8 respondents, will still have problem with Wi-Fi tracking.

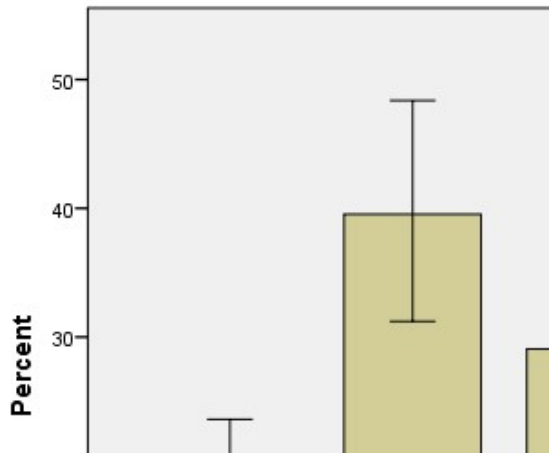
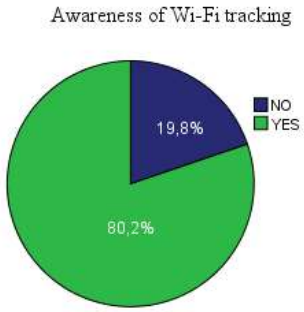
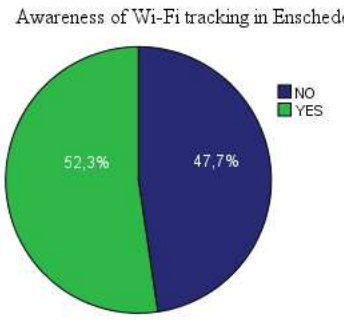


Figure 3 - transparancy

Question 4 of the survey is removed for analyzing the correlations. However, it is striking that almost 47% of respondents indicated that they would considering the opt-out option.





When comparing the difference between the groups who were already aware of Wi-Fi tracking and the group that was not aware, some slightly difference where found. Both groups worry about Wi-Fi tracking, but the group that is aware of Wi-Fi tracking scored a lower percentage on each question. Furthermore, the group that was not aware of Wi-Fi tracking before, tend to have a more negative outcomes when it comes to trusting municipalities and government. More that 47 % of the respondents that were not aware before, think that municipalities and government don't handle their data in the right way and with confidentiality.

V. ANALYSIS

The results showed that, more than 45% of the respondents weren't aware of the fact, that the municipality is using Wi-Fi tracking. This is consistent with Demir, (2013). Wi-Fi providers gathering mobile location data, consumers are being tracked, often without them knowing it. However, the results also showed that only 25% of the respondents was not yet knowledgeable with the concept of Wi-Fi tracking. It is specially the elder group respondents, that is aware of Wi-Fi tracking in the municipality. This could be explained by the fact that at the end of last year Wi-Fi tracking was in the news. One of the companies that was in the news was CityTraffic. There were privacy concerns do to their tracking behavior (Verlaan, 2016). Furthermore, studies of Demir, et al. (2014) and Michael, & Clarke, (2013), stated that Wi-Fi tracking can provide information on human dynamics such as the peoples paths, the crowd size, the visit duration and frequency and law enforcement utilize these technologies for surveillance. So this data is extremely valuable information for many applications. However the results of this study showed that almost 62 % of the respondents are not aware of the purposes of Wi-Fi tracking.

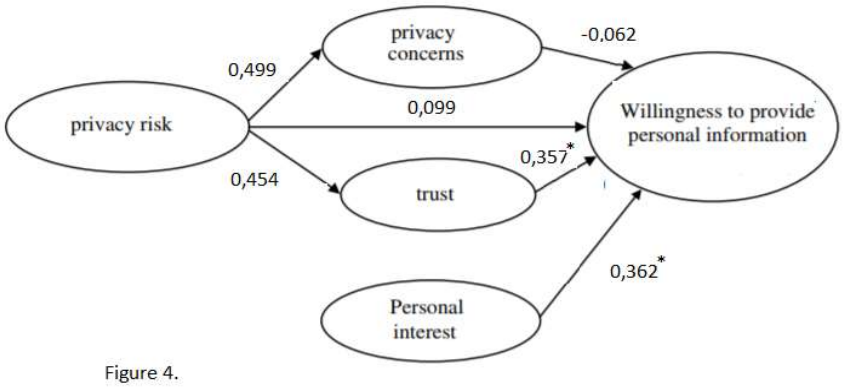


Figure 4.

Because of the lack of knowledge about the purposes of Wi-Fi tracking, most respondents don't know if they will experience (some) benefits of a better city or services, when municipalities are gathering their data with Wi-Fi tracking. However, most of the respondents think that Wi-Fi tracking is useful (54,7%). In the case of smart cities, governments and municipals can use the knowledge extracted to make strategic decisions and future city plans (Perera et al. 2014). Only 7% of the respondents stated that none of the purposes of Wi-Fi tracking will benefit them. The results showed that almost all respondents indicated safety as an important benefit of Wi-Fi tracking (86%). This is in line with the previous research of Heek, Arning and Ziefle, (2014). They found in their study that surveillance technologies are accepted, in those locations in which crime threat is present. Users then prefer safety over privacy. Furthermore, better facilities in the city are also seen as a possible benefit by 57%. According to previous research from Demir, et al.(2014), Wi-Fi tracking can enable urban planners to manage congestion and for better adaption of public spaces to citizens. Most respondents are indicating that the gathering of personal data comprises risks. And most respondents stated that they worry about the gathering and handling of their personal data. Possible misuse of personal data is the biggest concern of the respondents (60%). The results showed that the mean scores of the privacy are higher for females than for men, indicating that the group of females tend to have more worries regarding their privacy. This is consistent with the study of Fogel, and Nehmad (2009). In their research, women had significantly higher scores than men for privacy. Furthermore, Heek, Arning and Ziefle, (2014) stated that women attach a higher importance to safety in general, in contrast to men, while men prefer the protection of their privacy. Furthermore, This study shows that perceived risks, is not affecting the willingness to disclose information. No significant effect of risk and privacy on Willingness to disclose data has been found. Previous studies stated that people tend to be worried about their privacy when there is risk of sharing or the gathering of their data (Xu et al., 2009; Clarke 2001). So the results of this study are not really strange, when the analysis shows us that most of the respondents think there could be risks of losing privacy. However, despite the privacy concerns of people, the results of this study also showed that most of the respondents are willing to cooperate with municipalities when asked if they would comply. A possible reason mentioned in literature by Bailey, (2015) is that people are willing to trade-off their privacy because they are not fully aware when their private data are collected and are unaware of the amount of privacy that is being lost. So people are not aware about how exactly their data can be lost and how this will affect them. As a consequence of this conclusion, the validity of the privacy paradox in this specific context can be questioned.
Considering the fact that respondents of the questionnaire see risks in the gathering of data and still are willing to cooperate with Wi-Fi tracking, there can be doubts on what level people make-tradeoffs regarding Wi-Fi tracking and the possible benefits.

Previous studies have used the term “privacy calculus” to describe privacy-related behaviors and it has become a well-established concept in privacy research. Dinev and Hart (2006) advocate the use of a privacy calculus perspective whenever data disclosure, involves some degree of privacy risk. When disclosing personal data, individuals perform a simple risk-benefit calculation before deciding whether or not to disclose their personal information and against what costs. In the privacy calculus model used in this study, the variables privacy concerns, Risks, benefits and trusting beliefs are where integrated as key predictors of willingness to disclose.
Previous studies of the privacy calculus (Dinev and Hart 2006; Barth and de Jong 2017), found that privacy concerns and risks are on the negative side of the privacy calculus, and can prevent users from disclosing information. On the positive side, are the benefits, which motivates users to disclose information. The results of this study showed that, trust and benefits are the variables with significant positive determinants in the privacy model. So, this is consistent with the prior research of Dinev and Hart (2006). The cumulative effects of trust and personal interests can outweigh privacy risk perception to point that it eventually leads to the disclosure of personal information (Dinev and hart, 2006). This study showed that almost 47 % of the people are considering the opt-out option. Instead of being asked for permission, you must unsubscribe yourself from the City Traffic website so that it is not possible that municipalities or companies can track you. As mentioned before, previous research of Bosch and van Eijk (2016) suggests, that the continuous (de)activation of the phone or functionality can be a disproportionate effort. When municipalities, increasingly register Wi-Fi signals and hence peoples movements, it may not be desirable to put this responsibility entirely to the citizens.

The results of the privacy calculus furthermore showed, that risk had a very small positive, but non-significant effect on attitude, and a significant positive effect on trust as shown in figure 4. This is different with the previous study of Dinev and Hart (2006), who found that risks have a negative effect on trust. It could be that in general the population of this research have trust in municipalities to handle their data with care, in contrast to previous research, which focused on the trust in for example internet providers. Furthermore, some previous studies, have demonstrated that people rarely take a truly calculative approach to privacy decision making, and are often prone to take mental shortcuts instead (Acquisti and Jens Grossklags. 2005;Wilson and Valacich. 2012), which could be the case in the situation of Wi-Fi tracking. The study of Dinev and Hart (2006) also showed that, the more users experience privacy concerns, the more negative their attitude will be towards tracking of every kind. This is consistent with the results in this study. The more respondents experience privacy concerns towards WI-FI tracking, the less they are willing to comply with data disclosure. The results of this study showed that, 40 % of the respondents have no or less problems with Wi-Fi tracking, when they know how there data is gathered and how it will be used. Users should be informed about when and how data is gathered, what kind of data is gathered, what is happening to this data and whether data might be shared with third parties.

With the new GDPR, WI-FI tracking is bounded to specific laws and regulations as mentioned before. The result of the questionnaire showed that most of the people aren't negative on the statement, that existing laws and regulations protect their privacy. Laws and regulations are not sufficient for protecting residents, partly because of the fast moving technology society. Possible explanation for this is, that people probably don’t know exactly which laws are protection their privacy, but they probably tend to have general trust that there are enough laws to protect them from possible privacy violations.

VI. CONLUSION

Most of the respondents are knowledgeable with Wi-Fi tracking, but almost half of the respondents are not aware of the fact that the municipality is preforming Wi-Fi tracking. Furthermore, we can conclude that the people in the municipality are not aware of the purposes of Wi-Fi tracking.

People are willing to cooperate with municipalities when asked if they would comply. Despite of the negative sentiment of Wi-Fi tracking, most of the respondents want to comply with Wi-Fi tracking. Counter wise, most people also indicate that they are considering the opt-out option.

The majority of the responders tend to have trust in municipalities to handle their data with care and are not skeptical about the protection by the law. More trust can cause people to comply with Wi-Fi tracking. Trust can overrule the negative impact of privacy risk perceptions, what will benefit municipalities. This study confirmed the previous study of Dinev and Hart (2006). The results showed that Benefits and Trust had a significant and positive effect on the Willingness to disclose data.

The final conclusion is that the adoption of IoT is influenced by the privacy calculus, it is a balance between the benefits or value of the IoT, in this case security and improved logistics, and the risks involved, in this case loss of privacy. New privacy laws requires that Wi-Fi tracking requires consent. This gives people the freedom of choice and control over their personal data. Wi-Fi tracking can make an interference in the lives of people, therefore it is important that the Wi-Fi counting must be necessary and justified.

Although the number of responders is enough to generalize, the authors note that by applying it on just one municipality might bias the results. Further study in more cities is recommended.

REFERENCES

Acquisti and Jens Grossklags. 2005. Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy 3, 1: 26–33. https://doi.org/10.1109/MSP.2005.22

Al-Dhubhani, R., Mehmood, R., Katib, I., & Algarni, A. (2017, November). Location Privacy in Smart Cities Era. *International Conference on Smart Cities, Infrastructure, Technologies and Applications* (pp. 123-138).

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. I*nformation Systems Research*, *22*(3), 469-490.

Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805.

Bailey, M. W. (2015). Seduction by Technology: Why Consumers Opt out of Privacy by Buying into the Internet of Things. *Tex. L. Rev.*, *94*, 1023

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth?.*The Journal of Legal Studies*, *42*(2), 249-274.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online.*Decision support systems*, *49*(2), 138-150.

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011, December). Security and privacy in your smart city. In *Proceedings of the Barcelona smart cities congress* (Vol. 292).

Barkhuus, L. and A.K. Dey, "Location-Basedservices formobiletelephony: astudyofusers'privacyconcerns.," INTERACT. Citeseer, 2003, vol. 3, pp. 702–712.

Barth, S., & de Jong, M. (2017). The Privacy Paradox–Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review. *Telematics and Informatics*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly, 35(4), 1017-1042.

Beinat E (2001) Privacy and location-based services. Geo Informatics September. *Belissent, J. Getting Clever About Smart Cities: New Opportunities Require New Business Models, Forrester Research, 2010.*

Bosch, B. F. E., & van Eijk, N. A. N. M. (2016). Wifi-tracking in de winkel (straat): inbreuk op de privacy?. Privacy & Informatie, 19(251)

Chorppath, A. K., & Alpcan, T. (2013). Trading privacy with incentives in mobile commerce: A game theoretic approach. *Pervasive and Mobile Computing*, (4), 598-612.

Clarke, R (2001). Person location and person tracking: Technologies, risks and policy implications. Information Technology & People, 14, 2 (2001), 206–231.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115

Demir, L., Cunche, M., & Lauradoux, C. (2014, June). Analysing the privacy policies of Wi-Fi trackers. In Proceedings of the 2014 workshop on physical analytics (pp. 39-44). ACM.

Demir, L. (2013). Wi-Fi tracking: what about privacy (Doctoral dissertation, M2 SCCI Security, Cryptologyand Coding of Information-UFR IMAG).

Derikx, S., de Reuver, M., Kroesen, M., & Bouwman, H. (2015). Buying-off privacy concerns for mobility services in the Internet-of-things era. Proceedings of the 28th Bled eConference.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Elwood, S. and Leszczynski, A. (2011) Privacy reconsidered: New representations, data practices, and the geoweb. Geoforum 42: 6–15

Finch, K., & Tene, O. (2013). Welcome to the metropticon: protecting privacy in a hyperconnected town. *Fordham Urb. LJ*, *41*, 1581.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3-32). Springer Netherlands.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. Computers in human behavior, 25(1), 153-160.

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000). *The vision of a*

smart city (No. BNL--67902; 04042). Brookhaven National Lab., Upton, NY (US).

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.

Heek, J., Arning, K., & Ziefle, M. (2014, October). Safety and privacy perceptions in public spaces: an empirical study on user requirements for city mobility. In International Internet of Things Summit (pp. 97-103). Springer, Cham.

Heek, J., Arning, K. and Ziefle, M. Where, Wherefore, and How? - Contrasting Two Surveillance Contexts According to Acceptance. In Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2017), pages 87-98

Hernández-Muñoz, J. B. Vercher, L. Muñoz, J. A. Galache, M. Presser, L. A. Hernández Gómez, and J. Pettersson, "Smart Cities at the forefront of the future Internet," The Future Internet, Lect. Notes Comput. Sci., vol. 6656, pp. 447–462, 2011

Hollands, R. G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?. *City*, *12*(3), 303-320.

Könings, B., Schaub, F., & Weber, M. (2016). Privacy and trust in ambient intelligent environments. In *Next Generation Intelligent Environments (*pp. 133-164). Springer, Cham.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture.*Business & Information Systems Engineering*,*4*(3), 127-135.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*(6), 391-399.

Lee, H., & Kobsa, A. (2017). Understanding user privacy in internet of things environments. Paper presented at the 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, 407-412. doi:10.1109/WF-IoT.2016.7845392

Lee, J., & Rao, H. R. (2007). Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: an exploratory study of government–citizens online interactions in a turbulent environment. *Decision Support Systems*, *43*(4), 1431-1449.

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014, January). Privacy as a tradeoff: Introducing the notion of privacy calculus for context-aware mobile applications. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 1063-1072). IEEE.

Longo, S., & Cheng, B. (2015, September). Privacy preserving crowd estimation for safer cities. In Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (pp. 1543-1550). ACM.

Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. Future Generation Computer Systems, 75, 46-57.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Michael, K., & Clarke, R. (2013). Location and tracking of mobile devices: Überveillance stalks the streets. *Computer Law & Security Review*, *29*(3), 216-228.

Minch, R. P. (2015, January). Location privacy in the Era of the Internet of Things and Big Data analytics. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on* (pp. 1521-1530). IEEE.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

Mulligan C. and M.Olsson, "Architecturalimplications of smart city business models: An evolutionary perspective," IEEE Commun. Mag., vol. 51, no. 6, pp. 80–85, Jun. 2013.

Nam, T., & Pardo, T. A. (2011, June). Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times* (pp. 282-291). ACM.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. Transactions on Emerging Telecommunications Technologies, 25(1), 81-93.

Smith, H.J., S.J. Milberg, and S.J. Burke, "Information privacy: measuring individuals' concerns about organizational practices", MIS Quarterly, 1996, pp. 167–196

Steinfield, C. (2004). The development of location based services in mobile commerce. In *E-Life after the dot com bust* (pp. 177-197). Physica-Verlag HD.

Stewart, K.A., and A.H. Segars, "An empirical examination of the concern for information privacy instrument",

Information Systems Research 13(1), 2002, pp. 36–49.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(6), 16.

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the Association for Information Science and Technology*, *66*(5), 918-929.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), 615-624.

Westin, A. F., & Ruebhausen, O. M. (1967). *Privacy and freedom*(Vol. 1). New York: Atheneum.

Wilson, D.and Joseph Valacich. 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In ICIS 2012 Proceedings. Retrieved from http://aisel.aisnet.org/icis2012/proceedings/Resear chInProgress/101

Wirz, M., Roggen, D., & Troster, G. (2010, August). User acceptance study of a mobile system for assistance during emergency situations at large-scale events. In 2*010 3rd International Conference on Human-Centric Computing* (pp. 1-6). IEEE.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems, 26(3), 135-174

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.