# WIFI TRACKING IN THE IOT ENVIRONMENT OF SMART CITIES: A PRIVACY CALCULUS PERSPECTIVE

MASTER THESIS

KRYSTAN TEN BERG

UNIVERSITY OF TWENTE

SUPERVISORS: DR.IR. A.A.M.SPIL

DR. R. EFFING

ABSTRACT - *Over the last few years, we have seen the expanse of Internet of Things (IoT) solutions, products and services. The Internet of Things will capture a large amount of data pertaining to the environment, as well as their users. The real value of collecting data comes through data processing and aggregation in large-scale where new knowledge can be extracted. However, such procedures can also lead to user privacy issues. This study describes what people 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 Enschede. Demographic variables play a minor role. Gender and age differences where only found for privacy concerns and awareness of Wi-Fi tracking. Furthermore, the results showed 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 concerns, trust and perceived benefits significantly influence the willingness to disclose personal information. However, no significant effect of risk and concerns on Willingness to disclose data has been found.*

## I. INTRODUCTION

The smart city is critical for sustainable urban development. It could alleviate many critical problems accompanying the current overwhelming urbanization process, for example, traffic jams and environment pollution, using latest ICT technologies (Pan, Qi, Zhang, Li, Wu, & Yang, 2013). Smart city, along with big data, has grown in recent years by revolutionary technological developments in data collection, storage and processing. In this context, a wide range of smart city technologies are being deployed within the urban environments, and all of these technologies generate huge quantities of (real-time) data. This data is important for all smart city applications. But the absolute dependence human life has on reliable information & communication technologies, will create issues related to privacy and security to emerge.

Since a couple of years, Dutch cities started with utilizing monitoring technologies. Monitoring, understanding and predicting city user behavior (hottest places, trajectories, flows, etc.) is one the major topics in the context of Smart City management. By leveraging citizen's mobile devices to measure environmental context, mobile crowd sensing becomes a central part of any smart city (Shin, Cornelius, Kapadia, Triandopoulos, & Kotz, 2015).

The collection and analysis of data in the IoT applications has many objectives. Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). 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; Asin & Gascon, 2012). However, IOT comes with certain disadvantages as well. Foremost is security and privacy. All these devices collect lots of personal data and unless it is not encrypted, it can be shared and misused by known or unknown. With these new technological developments, it is now easier for governments and companies to collect and use data from citizens. Not least is the worry that an increase in data-gathering sensors and cameras in urban areas amounts to excessive government surveillance, which could increases the possibility for public dissent. An example of this is China, where there are big data policing platforms that aggregate and analyze massive amounts of citizens' personal information, The system is designed to track and predict the activities of activists, dissidents, and ethnic minorities, where China has no enforceable protections for privacy rights against state surveillance.[1]

The differing levels of privacy concern can cause a change in attitude. The more worried users are about the safety of their personal information, the more negative they will feel towards the collection of location data. However, change in attitude does not always result in a change in behavior. In some cases, people might not take action because of a lack of motivation or knowledge (Ketelaar & van Balen, 2018). The Location privacy preference of users has not been studied extended through an IoT context where device-to-device communication can carry location information far beyond users' awareness (Minch, 2015).

As part of their Smart city agenda, Enschede started Wi-Fi tracking in September of 2017[2]. Tracking data are used to see how the city functions. Where do visitors walk, which routes do they take, how long do people stay in the city center and how often do they return. By gathering these data from visitors, the

1 https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

2 https://www.enschede.nl/bestuur/privacy/wifi-tellingen-binnenstad

city get resources to maintain or improve the attractiveness, security, accessibility and liveliness of the cities. To find out what the awareness of being tracked has on the sense of privacy and how trust, perceived risks, concerns and benefits can influence the Willingness to disclose data, this thesis will use the privacy calculus model to find relations between these constructs.

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 research the focus will lie on the privacy calculus and Wi-Fi tracking. So far, there has been no earlier research, which has tried to understand consumers' attitudes towards this specific form of data collection. This research is not only important to investigate citizens attitudes towards being tracked, but also how these attitudes relate to actual behavior. This paper will give answer to the following research question: *Are citizens of Enschede aware that they can be tracked and how can the elements risk, concerns, trust and benefits, as used in the privacy calculus, affect their attitude to data disclosure.*

The structure of the thesis is as follows. First the method of this research will be described. Followed by a short introduction about smart cities and the internet of things. Furthermore, the principle, applications and privacy issues of Wi-Fi based tracking systems are described. Followed by the constructs of the privacy calculus. §VI. concludes this paper.

## II. METHOD

The objective of this study is to learn the pre-existing level of awareness that the participants hold regarding Wi-Fi tracking and derive to their core beliefs in order to understand what elements of the privacy calculus lead to the privacy concern and their attitude towards data disclosure. The base of this research will consist of qualitative research. The approach for this study is based on an in-depth literature review of relevant studies as well as official documents of international institutions. The literature study is conducted with data bases such as Scopus, Google scholar, Sciencedirect, Web of science and Jstor. Keywords used to find articles related to the topic are, privacy calculus, WIFI tracking, Privacy concerns, 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 amount 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 key word “privacy calculus“ provided 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.

The motivation behind investigating the tracking and monitoring privacy issues in smart cities, is the increasing use of IOT sensors in smart cities in the Netherlands. These sensors can enhance citizens privacy concerns. Literature study showed that there are different kinds of privacy issues which can arise with the deployment of IOT sensors for monitoring purposes. It also made clear that people are willing to share personal data, depending on the benefits that they can gain. The literature regarding privacy is grounded on the privacy calculus. This theory is used to describe the drivers between the perceived benefits, the privacy risks and users’ perception of privacy and their concerns with data gathering in the connected object space.

*Data Collection – Questionnaire*

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 Enschede, 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. In this study, citizens of Enschede are naturally a part of the population of interest.

The survey was distributed and participants were recruited in several ways. The online survey was first send to acquaintances by mail. The researcher asked them to fill in the survey and also to spread the survey in their networks. Furthermore, the survey has been distributed face to face in Enschede. To got the attention of possible participants and to made it more appealing to participate, every participant could win one of two bol.com vouchers. The survey was translated from English to Dutch and then back to English following a generally accepted practice to ensure consistency in cross-lingual surveys (Karahanna et al., 2002). Most scales in this study were based on a five-point Likert scale, as has been used in previous research involving the privacy calculus. The Likert scale is used to make the constructs of the privacy calculus measurable, which are normally difficult to measure in quantitative research. The scales are ordered as follow, where 1=fully disagree and 5=fully agree. This study revolves around the variables: Awareness towards Wi-Fi tracking, Privacy concerns, Privacy risks, Trust, Personal interests (benefits) and Attitude towards Wi-Fi tracking.

To ensure construct validity, scales from previous studies will be adapted wherever possible. The survey consist elements taken from the privacy calculus of Dinev and hart (2006) and Barth and de Jong (2017). The actual items were slightly modified from the original instruments to capture the 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). Trust will be adapted from Dinev & Hart (2004, 2006);Malhotra et al. (2004); and Westin (2001), attitudes to disclose will be assessed using scales adapted from Anderson and Agarwal (2011). It will also include demographic variables such as age, gender. To prevent bias towards a negative or a positive attitude, the survey questions are formulated positive and negative, depending on the construct. The outcomes of the survey are analyzed using SPSS. Measure validation for reliability was established through examining Cronbach’s alpha coefficient for each construct. Relations between the different constructs are analyzed with correlation and regression analysis. Because of the limited respondents for the analysis a 90% confidence interval is chosen.

The administrated survey is found in appendix C

## III. LITERATURE

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

*Smart-cities*

Recent literature revealed that descriptions of smart cities are now including qualities of people and communities as well as ICTs (Albino, Berardi, & Dangelico, 2015). According to Giffinger and Gudrun, (2010) is a Smart City a well performing city built on the 'smart' combination of endowments and activities of self-decisive, independent and aware citizens". Neirotti, Paolo, De Marco, Cagliano, Mangano and Scorrano, (2014) found in their study that Smart cities are a wide notion that encompasses many different socio-environmental aspects and ICT applications. Belissent (2010), stated that the Smart city is the one that uses information and communications technologies to make the city services and monitoring more aware, interactive and efficient. Smartness of a city is driven and enabled technologically by the emergent Internet of Things (IoT) (Atzori, Iera and Morabito 2010).
According to Nam and Pardo (2011), the concept of a Smart city is an organic connection among technological, human, and institutional components. Nowadays the usage of "smart" captures innovative and trans-formative changes driven by new technologies. However, social factors other than smart technologies are central to smart cities. The "people" domain emphasizes innovation, learning resources, and human capital that serve as catalysts to boost Smart City development. The institution domain indicates the importance of government support in the development of Smart Cities. And the technology domain addresses the need to build basic infrastructure, both physical (hardware) and virtual (wireless networks), to implement information-communication technology in urban areas (Zhang, 2017). 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".

*IOT*

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, economical and technical implications the full deployment of IoT will have. They furthermore stated that, the reason of today apparent fuzziness around this term is a consequence of the name ''Internet of Things" itself, which syntactically is composed of two terms. The term "Internet of Things" (IoT) refers to ubiquitous networking; where all things or objects are connected to each other via wired or wireless communication networks (Aleisa & Renaud, 2017). Billions of devices are connected to the network and have the ability to sense, compute, communicate and act and thus intelligently become part of the Internet (A. Zaslavsky, C. Perera & D. Georgakopoulos, 2013; Coetzee & Eksteen, 2011). The communication among all these "things" is referred as Internet of Things (Said and Masut, 2013). This is consistent with Mukhopadhyay and Suryadevara (2014), who stated that the Internet of things is used to describe embedded devices (things) with Internet connectivity, allowing them to interact with each other, services, and people on a global scale. The definition of "things" is very wide. Things include personal objects we carry around such as smart phones, tablets and digital cameras. It also includes elements in our environments as well as things fitted with tags which become connected via a gateway device (e.g. a smart phone) (Coetzee & Eksteen, 2011). These enormous number of devices and things that are connected to the Internet, will provide data and information and some, even services. Data and data-related processes such as generation, acquisition, transmission, and interpretation are central drivers in the design and application of IoT. Without data, IoT does not exist (Weinberg, Milne, Andonova & Hajjat, 2015). Zanella, Bui, Castellani, Vangelista, and Zorzi (2014) state that, enabling easy access and interaction with a wide variety of devices, the IoT will foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services to citizens, companies, and public administrations. 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.

*Relationship between Smart-city and IOT*

Earlier in this study it was noticed that there are a set of core factors underlying the smart city concept. 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.

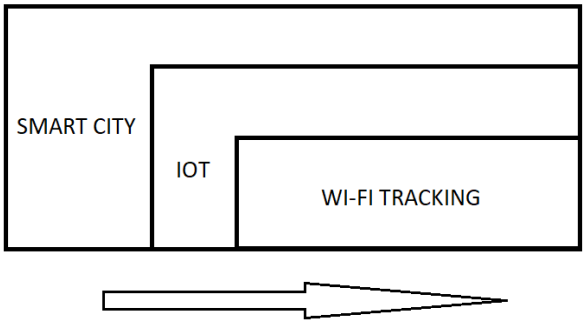



Fig.1

The 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. 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). Compared to the Web era, the IoT is more vulnerable to privacy violations. Previous research highlighted the fact that privacy concerns 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.

*Applications of IOT: Wi-Fi & bluetooth tracking*

According to Zanella et al,. (2014), will the IoT by enabling easy access and interaction with a wide variety of devices such as, for instance, home appliances, surveillance cameras, monitoring sensors etc, foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services. One of these applications is Wi-Fi tracking. The rapid deployment of smart-phones as all-purpose mobile computing systems has led to a wide adoption of wireless communication systems such as Wi-Fi and Bluetooth in mobile scenarios (Schauer, Werner & Marcus 2014). Wi-Fi has become so ubiquitous. You can find it at stores, hotels, airports, hospitals, etc. Up until recently tracking the movement of individuals was a slow process. However, smart technologies has transformed geo-location tracking to a situation where the monitoring of location is pervasive, continuous, automatic and relatively cheap, it is straightforward to process and store data, and easy to build up travel profiles and histories (Kitchin, 2016).

Pang, Greenstein, Gummadi, Seshan and Wetherall, (2007) stated that it is trivial to track a device today since each device advertises a globally unique and persistent MAC address with every frame that it transmits. So, Wi-Fi trackers stores and processes location data with the Media Access Control (MAC), the unique identification number of your mobile device, such as a smart-phone. It may be a MAC address or radio-frequency identification (RFID), which is a technology that uses communication through the use of radio waves to exchange data between a reader and an electronic tag attached to a device for the purpose of identification and tracking it (Mena, 2013). Mobile devices can be traced in three ways: via mobile signals, via blue-tooth and via Wi-Fi. The mobile device does not necessary need to be connected to a Wi-Fi network to be tracked. Trackers rely on the MAC address to uniquely identify each individual. By collecting radio signals emitted by Wi-Fi enabled devices, those systems are able to track individuals and will provide information about the crowd density in cities (Schauer et. al, 2014). MAC address data allows for unannounced, non-participatory, and simultaneous tracking of people.

A trace generated by a moving object, is usually described by a temporal sequence of spatial points with their timestamps. It conveys underlying information on people and cities, such as traffic, human activity, and social events (Pan et al., 2013). With a sufficient number of sensors, an almost complete profile of a person's movement in a city can be obtained. Although identity is usually not revealed directly in the form of a name, a recurring network identifier such as a network MAC address can provide the association. The MAC address act as a pseudonym for the tracked individual (Cunche, 2013). However, even though the MAC address does not directly reveal the identity of a person, the fact that it is constant over time and easy to intercept, means that it can be used for recognizing individuals between different sensor points and tracking their movements. Moreover, most people live at a fixed address they return to each evening, and this address can be easily linked with a person's name. Therefore, as you continue to use your smart device at home with other networked devices, you could inadvertently link your name with the MAC address, thereby also potentially revealing your location history (Want & Dustdar, 2015), which as consequence make people vulnerable to a range of privacy breaches (Cunche, 2014).

*Purposes of Wi-Fi tracking*

Trace analysis and mining can exact and reveal inherent information or knowledge about a city and its people. It will benefit broad applications, such as transportation, urban planning, public health, public security, and commerce (Pan et al 2013). The need to capture and predict location data of individuals and crowds is crucial for urban traffic monitoring, predicting future localized demands of network usage and crowd management (Haas, 2016). Wi-Fi tracking enables urban planners to manage congestion and for better adaption of public spaces to citizens. It also gathers important data on pedestrian behavior and their destination preferences. Knowing human dynamics such as the people path, the crowd size or the visit duration and frequency are extremely valuable information for many applications (Demir, et al.2014). Furthermore, are citizens also increasingly being monitored and tracked for commercial interests. Many organizations want to benefit from the use of Wi-Fi tracking. Hochheiser, (2015) provided in their research examples, of shops that used Wi-Fi tracking techniques to generate business-related information. These shops gathered data about how many people passes the store, how many visitors enter the store etc. These stores wants to use Wi-Fi tracking to determine where shoppers lingered and to get a better sense of customer foot traffic. After obtaining this information, the example store can modify its marketing strategies to conform to what shoppers want by tracking the time they spend at certain displays (Hochheiser, 2015).

Tracking and monitoring enables a range of applications for smart cities, such as localization and tracking of objects, healthcare applications, asset management and smart parking (as cited in Hancke, & Hancke Jr, 2012). Municipalities and event organizers, for example, use the technique to map downstream streams and keep track of how long visitors stay in a particular place[3]. In addition, law enforcement utilize these technologies for

3 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-winkels-en-gemeenten-op-

surveillance, can do so inexpensively and hence can track many more people (Michael, & Clarke, 2013). People flow surveillance provides valuable information about city conditions, useful not only for monitoring and controlling the environmental conditions, but also to optimize the delivering of city services (security, clean, transport, etc.)

*Privacy threats*

At first sight, little seems wrong with governments wanting to use techniques for optimizing their cities. With the help of tracking data, they can take measures based on hard facts and they can intervene faster if anything goes wrong. But, despite the fact that retailers and business have high expectations for physical tracking, it is also a threat for citizens privacy (L,. Demir M. Cunche C. Lauradoux, 2014). This is because the traces provide important information on the mobility of moving objects (Pan et al. 2013). The Wi-Fi access points, can be used then to know something about pedestrian behavior.

In many mobile crowd-sensing applications, knowing the identities of the devices is unnecessary (Shin et al. 2015). Unfortunately, knowing a user's locations (coupled with the knowledge of their historical movement patterns) is often enough to de-anonymize data (as cited by Chin et al., 2015). By recording the whereabouts of any individual that happen to carry a device with Wi-Fi turned on, they can monitor the activities of a large fraction of the population. Therefore, it is impossible for the user to know if whether or not tracking is performed (Demir et al. 2014). Furthermore, through the digitization of many services and information, personal information is stored on vast databases owned by both companies and governments. This increases the possibility of a user's privacy being compromised. Ketelaar, P. E., & van Balen, M. (2018). So the deployment of tracking and monitoring technologies in smart cities, can possible raise privacy concerns by citizens. Therefore, such data must be managed carefully to avoid any user privacy violations.

*Laws and regulations*

Research around tracking and monitoring of humans has been sensitive to the privacy and ethical problems surrounding the topic. Smart cities, at least in Europe, will still suffer as a project if they fail to get privacy right (Edwards 2016). Privacy legislation tries to draw boundaries to the evermore data-hungry business models of many Internet enterprises and to define mandatory practices and processes for privacy protection. The development and practical impact of privacy legislation will be shortly described.

Recently, CityTraffic was in the news because there where privacy concerns in the way they where tracking smart phones (Verlaan, 2016). Citytraffic is a company which performs tracking for municipalities and companies. In order to monitor citizens, municipals and companies need to be compliant to the General Data Protection Regulation (GDPR). Since the 25th of may 2018 the GDPR became an enforceable law. Dutch personal data Protection authority (Autoriteit persoonsgegevens) is the central independent authority that monitors the compliance with the rules of the GDPR. The authority investigates the use of personal data within companies and government organizations. The GDPR implements the protection of individuals with regards to the processing of personal data.

Organizations may only process these personal data in accordance with the General Data Protection Regulation (GDPR) if they have a so-called legal basis. A personal basis is required for the processing of personal data. Municipalities have to perform a public task and they may process personal data in that context. An organization may also use Wi-Fi tracking if this is necessary for service. This also applies to organizations with a public-law task, such as municipalities, or if there is a legitimate interest: "Those organizations can process personal data through Wi-Fi tracking if necessary to perform that task." In addition, only in those periods and in areas where it is really necessary can be measured.

The one form of wifi tracking is a lesser privacy violation than the other. A higher risk exists, for example, when people follow for a longer period of time. Under the GDPR, wifi tracking would usually require permission, except in a number of exceptional cases. For example, if you only count the number of visitors in a city, and the data are anonymized immediately upon receipt. Or when you use data purely for statistical purposes, then immediately discard or anonymize it, and there is an effective opt-out to users. Other forms of Wi-Fi tracking may be allowed, when permission is provided by people before the tracking takes place. The Dutch personal data protection authority, warned that Wi-Fi tracking without informing the people, is in violation with the law. Additionally, people are not required to give permission and may withdraw permission. Furthermore there is a retention period. The data may no longer be stored in a form that allows the person (s) to identify than necessary for the implementation of Wi-Fi tracking purposes. A MAC address in combination with location data may be stored for up to 24 hours when this is necessary for the service. [4] Regulatory law states that data may only be disclosed if they are not traceable to an individual. But as soon as data will be combined, they are quickly redirected to individuals. Which is not desirable.

Personal data can be defined as followed: "any data relating to an identified or identifiable natural person". The protection of privacy is a fundamental right. According to the GDPR, is data that can be direct or indirectly be traced to a person, are considered as personal data. So indirectly identifiable data are also personal data.
Bosch and van Eijk (2016) suggests in their research, that the question remains whether it should be left to the consumer to conduct an active act to withdraw from Wi-Fi tracking by indicating an opt-out or disabling of its devices. Increasingly, consumers and pedestrians use devices that deliver Wi-Fi signals that can be registered. When retailers as well as communities in the context of smart-cities, increasingly register these signals and hence the consumer's displacement behavior, it may not be desirable to put this responsibility entirely to the consumer. This is as well put by the AP. They stated that the continuous (de)activation of the phone or functionality is a disproportionate effort.

Laws and regulations are not sufficient for protecting citizens, partly because of the fast moving technology society (Levenbach, 2017). And even if technological applications may fit into the frameworks of the law, it may have a negative impact on the concerns of people or society as a whole. Legislation is about what organizations can do with data, but ethics should tell us what organizations should do with data.

## III.II PRIVACY IN THE INTERNET OF THINGS PARADIGM

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

voorwaarden-wifi-tracking Geraadpleegd op 19-09-2017

4 http://www.socialmediatoday.com/technology-data/adhutchinson/2015-06-05/convenience-vs-privacy-latest-study-data-tracking-debate

from the environment and will share them with other devices and backend servers (Lopez, Rios, Bao & Wang, 2017).

*Monitoring and privacy concerns*

Tucker, (2012) stated, that in essence people are concerned about the lack of control over their personal data. 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 surrounding, 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, 2014). 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, 2016). In fact IoT and Ubiquitous technology are leading to increasing privacy concerns as they are capturing and storing more and more information about people and their activities (Longo and Cheng, 2015).

*Defining privacy*

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 concern acceptable practices with regards to accessing and disclosing personal and sensitive information about a person (Elwood and Leszczynski (2011).

With the increasing use and efficiency of electronic data processing, information privacy has become the predominant issue today (Ziegeldorf, Morchon and Wehrle, 2014). According to Kitchin, R. (2016), personal and sensitive information can relate to a number of a personal facets and domains creating a number of inter-related privacy forms including:

•Transactions privacy (to protect against monitoring of queries/searches, purchases, and other exchanges)
•Identity privacy (to protect personal and confidential data);
•Bodily privacy (to protect the integrity of the physical person);
•Territorial privacy (to protect personal space, objects and property);
•Locational and movement privacy (to protect against the tracking of spatial behavior);
•Communications privacy (to protect against the surveillance of conversations and correspondence).

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 WIFI 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*

Gassen & Fhom (2016) 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. This is consistent with Demir, (2013). He stated that most people are unaware that their Wi-Fi is a potential source of tracking. 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. (Medaglia and Serbanati, 2010). Furthermore, Fife and Orjuela, (2012) stated that it is clear that users are not fully aware when their data such as age, gender, habits, address, and other items are collected, aggregated or possible sold to a third party. 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.*

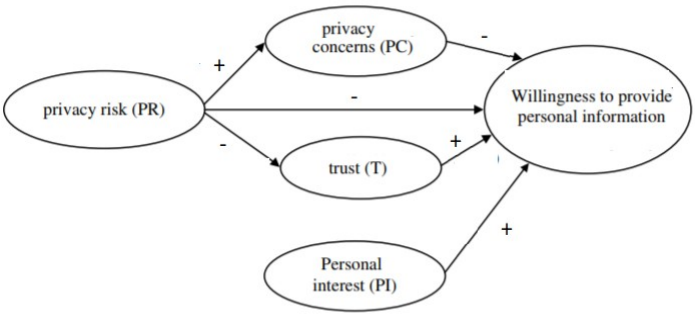



*Fig. 2 Privacy calculus (Dinev and Hart 2006)*

The discrepancy between actual or intended privacy related behavior and stated privacy concern is coined as the privacy paradox. Wilson et al., (2012) stated that, the privacy calculus is a possible explanation for the privacy paradox. The privacy paradox is know as the discrepancy between the expressed concern and the actual behavior of users. In other words, people claim to be very concerned 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 concern 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 (Levenbach, 2017). 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 individuals 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 concerns 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.

## IV. RESULTS

A. Descriptive statistics

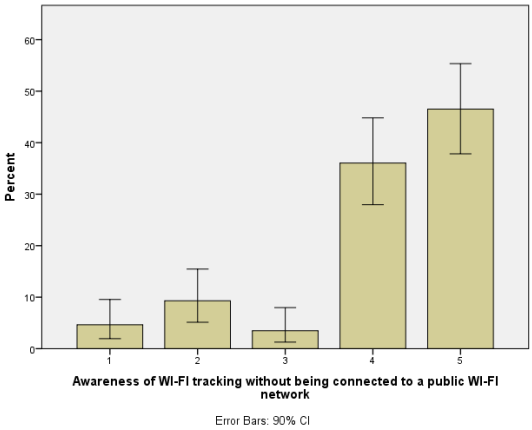
The total amount of respondents is 86. All responses were valid with no missing answers. The distribution of male and female respondents was N= 51 and N=35. The Mean age was 34.56 (SD = 11.74). For the analysis the difference between male and female and age groups are taken in to account. For the most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

The graphs in figure 3 display the awareness of Wi-Fi tracking in general and in Enschede. From the descriptive analysis, it shows immediately 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 wasn't 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%.



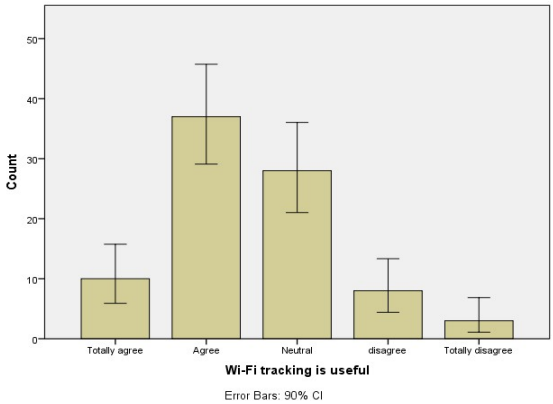

Most respondents don't know if they will experience (some) the benefits of a better city or services, when municipalities are gathering their data with Wi-Fi tracking. But most of the respondents think that Wi-Fi tracking is useful (54,7%).
Almost all respondents have chosen safety in cities as a possible 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

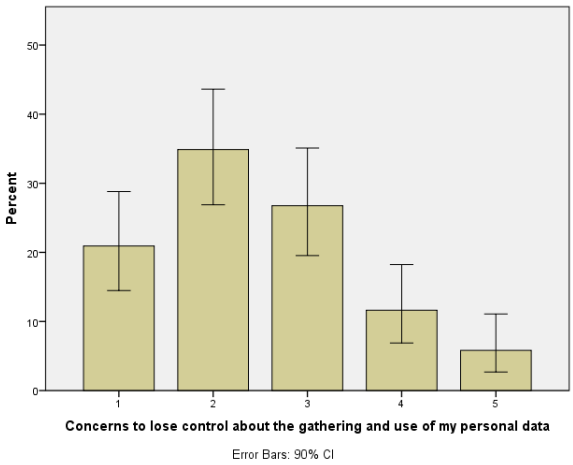


In general the respondents do trust municipalities and government to handle personal data with confidence. There is no exception between the younger group of respondents (<42 and the older group (>43). However there is a difference between males and females. Males tend to have higher trust in how municipalities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

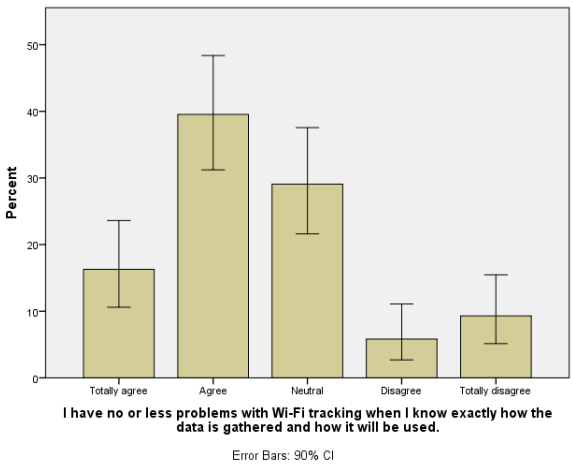
Most respondents are indicating that the gathering of personal data comprises risks. And most respondents stated that they have concerns about the gathering and handling of their personal data. Possible misuse of personal data is the biggest concern of respondents (60%). The results showed that the mean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

| | N | Mean | Std. Deviation |
|---|---|---|---|
| latent_concerns | 35 | 3,8357 | ,94118 |
| Valid N (listwise) | 35 | | |
| latent_concerns | 51 | 3,2745 | ,93308 |
| Valid N (listwise) | 51 | | |

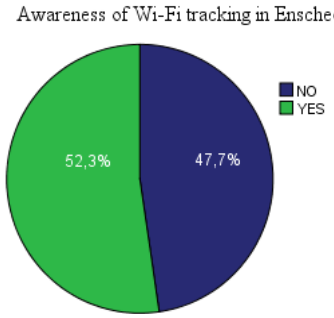
Like the concerns, more than 51 % see the misuse of personal data as a (very) high risk. Actually, all the elements of risk are considered (very) high risks by respondents. Furthermore, most respondents (56%) have concerns that they will lose control about how their data is gathered and used (see graph appendix A). In the open comment section respondents indicated, that the possibility of their data being hacked is also a big risk.

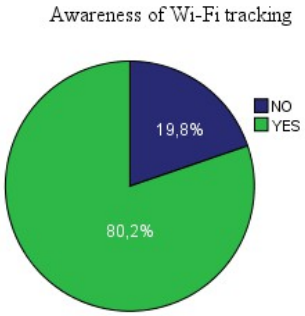



Almost 40 % of the respondents indicated that they have no or less problems with Wi-Fi tracking, when they exactly know how there data is gathered and how it will be used. Only N=8 respondents, will still have problem with Wi-Fi tracking.

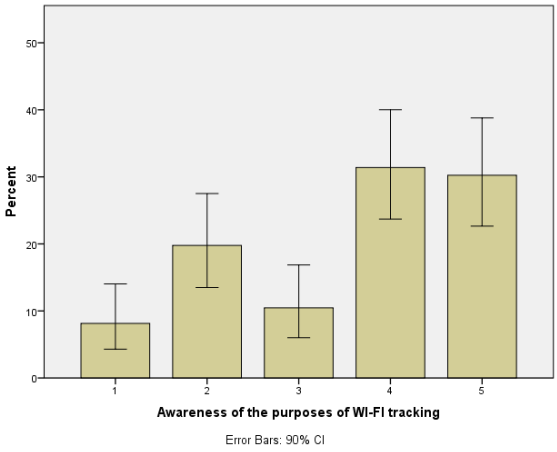



Question 4 of the survey is removed for analyzing the correlations. However, it is striking that almost 47% of respondents indicated that they would considering the opt-out option.




When comparing the difference between the groups who where already aware of Wi-Fi tracking and the group that was not aware, some slightly difference where found. Both groups have concerns 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.




B. ANALYSIS

The reliability of Likert-type scales can be checked using Cronbach's Alpha α (internal consistency). In general, a value of 0.7 and up (the ceiling is 1.0) means good internal consistency. Conceptually, it measures how well the items function together (e.g., do people respond consistently with their standing on the construct of interest) Most scales exceeded the recommended thresholds of .70 for Cronbach's α and composite reliability (Gefen et al., 2000). However there where two exceptions for the scales benefits and attitude. At both scales item(s) had to be removed in order to get a higher Cronbach's α. Some composite reliability coefficients were even above. 80, indicating strong internal consistency (Koufteros, 1999).

CORRELATIONS
A correlation matrix shows the initial relations between variables, and provide a clear overview. The privacy calculus model is first checked for normality to determine the type of correlation matrix. A Shapiro-Wilk test proved the data to not be normally distributed (Sig<0,05) and therefore, a Spearman correlation matrix is used for non-parametric tests. The full correlation matrix can be found in Appendix A. The highest significant correlations to the dependent variable Attitude is reported in Trust (,623**), followed by Benefits (,620**). Followed by Risk (.349**) and concerns (.326**). This suggests a strong influence of Trust and Benefits on Attitude at first glance. There are no high inter-item correlations (>0,7) found. Negatively formulated questions are reversed before taken into account in this correlation matrix. The rest of the correlations between items can either be qualified as low (0,3 to 0,5) and moderate (0,5 to 0,7) correlations. This shows that the items are somewhat related.

| |
|---|
| 0,779 α Benefits 1 item removed |
| 0,881 α Trust |
| 0,842 α Risks |
| 0,906 α Concerns |
| 0,767 α Attitude 2 items removed |

REGRESSION
The regression analysis are used to check for significant coefficients. The first regression analysis was run to predict the influence of Perceived risks, Perceived benefits, Perceived concerns and Trust on the Willingness to disclose personal information (attitude). The assumptions of independence of errors, linearity, homoscedasticity, unusual points and normality of residuals were met. $p<0.000$, $R^2=.462$. The regression coefficients and standard errors are shown in the table of appendix B.

As the privacy calculus model of Dinev and Hart was examined, the results only revealed two significant coefficients at a 0,10 alpha level. Trust and benefits (Sig<0,10) are the variables with significant determinants in the privacy model. This model (See figure 4) shows that there are no significant coefficients of the assumed significant variables concerns and risks. This is at odds with the model presumptions. Furthermore, privacy risks shows a significant effect on privacy concerns, with an estimate of 0,499.

Finally, significant results are found for Trust and Benefits on Willingness to disclose / attitude.

## V. DISCUSSION RESULTS

The results showed that, more than 45% of the respondents wasn't aware of the fact, that the municipality of Enschede is using Wi-Fi tracking. This is consistent with Demir, (2013). Wi-Fi providers gathering mobile location data, consumers are being tracked, often without they knowing it. However, the results also showed that only 25% of the respondents was not yet known with the concept of Wi-Fi tracking. It is specially the elder group respondents, that is aware of Wi-Fi tracking in Enschede. 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. They where in the news because there where 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

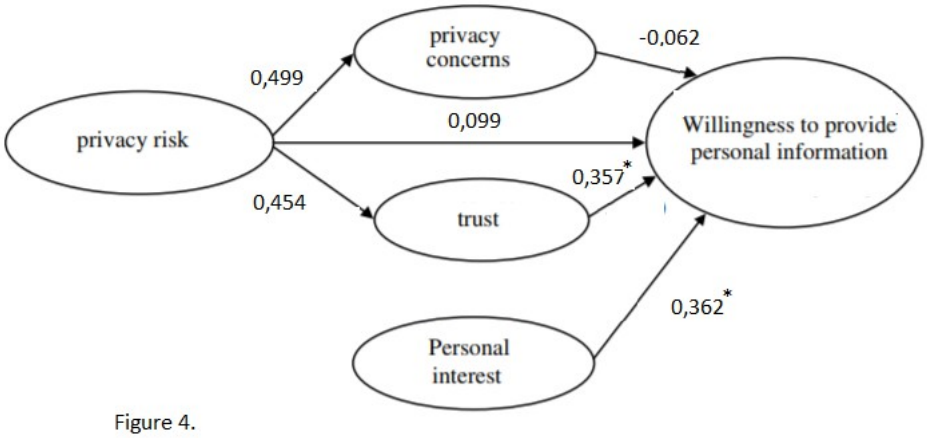



Figure 4.

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.

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; Asin & Gascon, 2012). 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 have concerns 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 concerns are higher for females than for men, indicating that the group of females tend to have more concerns 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 concerns. 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.

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)

Furthermore, This study shows that perceived risks, is not affecting the willingness to disclose information. No significant effect of risk and concerns on Willingness to disclose data has been found. Previous studies stated that people tend to be concerned 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 their 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 Fife and Orjuela, (2012) and 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 have concerns, 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-trade offs regarding Wi-Fi tracking and the possible benefits.

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. 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. Gassen & Fhom (2016) stated in their study, that companies should improve awareness & transparency of data practices as a solution to handle privacy issues. 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. In the study of Levenbach (2017) was mentioned that 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.

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.

## VI. CONLUSION

The goal of this study was to integrate theories and research from The privacy calculus and Wi-Fi tracking to create a preliminary research which will give an explanation for the privacy paradox and provide an overview of the attitudes of citizens towards Wi-Fi tracking in cities. People often claim to be very concerned about their privacy but do very little to protect their personal data. To analyze this privacy paradox, the relationship between Privacy concerns and Willingness to disclose personal information was measured.

The variables privacy risks, privacy concerns, trust and perceived interests are measured to explain the attitudes of citizens towards the willingness of disclosing of personal information and to give a possible explanation for the privacy paradox. The aim of this study was to provide an answer on the following research question: "*Are citizens of Enschede aware that they can be tracked and how can the elements risk, concerns, trust and benefits, as used in the privacy calculus, affect their attitude to data disclosure.*"

The first conclusion of this study is, that most of the respondents are known with WI-FI tracking, but almost half of the respondents are not aware of the fact that the municipality of Enschede is preforming Wi-Fi tracking. As mentioned before, Wi-Fi tracking without informing the people, is in violation with the law. Enschede recently (mid of January 2018) placed signs near the city center, that they are performing WI-FI tracking. The signs are placed at the access roads to the area where the WI-FI signals are measured. The high percentage of people who are not aware of WI-FI tracking in Enschede, can maybe be explained because of the overlap between the survey period and the placing of the signs. It is possible that citizens didn't notice the signs yet, or the signs are not visible or notable enough.

Furthermore, we can conclude that the people in Enschede are not aware what the purposes of Wi-Fi tracking are. Municipalities should consider this as a point of attention. Prior literature as well as this research, concluded that municipalities should inform citizens properly or involve them in the process of gathering data, because most of the respondents are willing to cooperate with WI-FI tracking when they know how and when their data is gathered and used. If people find the use of tracking technologies useful for public purposes, it is easier to accept it.

This research also concluded that, 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 wants to comply with Wi-Fi tracking, The lack of awareness and the fact that people see enough benefits of the use of Wi-Fi tracking, can strengthen this effect. But in opposition, most people also indicate that they are considering the opt-out option. However a lack of transparency and awareness may undermine the ability of the citizens to effectively anticipate at privacy risks associated with the collection and processing of their data, and to subsequently take adequate countermeasures.

Furthermore, this study showed that people 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.

And as final conclusion, 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 tot disclose data (Attitude). However, it failed to confirm that perceived risks, is affecting the willingness to disclose information. People have concerns about the gathering of data, but from the results of this study we can conclude that the benefits overrule the concerns. Creating trust and providing citizens with a clear overview of the benefits of Wi-Fi tracking, can prevent negative sentiment by citizens. However, considering the fact that respondents despite the perceived concerns and risks are still willing to cooperate with Wi-Fi tracking, there can be doubts on what level people make-trade offs regarding in the context of Wi-Fi tracking.

## V.II IMPLICATIONS

This study expands on existing knowledge by exploring users' privacy concerns and their awareness of Wi-Fi tracking. This study provides useful information for both citizens of Smart cities as for Municipalities. It is important for citizens to realize that their privacy concerns maybe grounded. Tene & Polonetsky, (2012) stated that privacy in the era of big data, causes information off individuals in the smart city is exposed to analysis, sharing, and misuse, which is a condition that gives rise to concerns about profiling, stealing, and loss of control. This study, combined with previous research, shows that people have privacy concerns and want to control the access that municipalities have to their personal data as much as possible. This is important for municipalities to recognize, as they are the ones collecting information about citizens with Wi-Fi tracking. If people respond negatively to tracking of their data, their attitude to comply will continue to decrease and trust in municipalities will decrease to.

Tracking can be undesirable and offensive, especially if people are unaware of it and for which purposes it is done. Tracking without informing people, has privacy implications as people will lose control over their own personal data and are no longer able to exercise their right to make informed choices. A fundamental principle of privacy is that the collection of personal data should not take place covertly. Because most of the concerns of people are losing control about the way personal data is gathered and used by municipalities, they should keep location tracking transparent and gather information within limits, making data disclosure more a choice that can be made, and giving people the feeling that they are in control of their privacy. Municipalities and organizations, should recognize that they do not own peoples data. Knowledge about WI-FI tracking can also be improved, by explaining it in more detail. People may lack the skills and knowledge to protect their privacy.

New privacy laws requires that Wi-Fi tracking requires consent. This gives people the freedom of choice and control over their personal data. However, it must be noted that only simple counting can take place when it is necessary to carry out a legitimate interest that possibly outweighs the individual's right to privacy. Because Wi-Fi tracking can make an interference in the lives of people, it is important that the Wi-Fi counting must be necessary and justified.

## VIII. LIMITATIONS AND FUTURE RESEACH

An important note regarding this study is its representativeness. The results are applicable to the specific group (citizens of Enschede) of the population which formed the sample. This makes it difficult to definitely generalize the results to other cities or the full Dutch population. However, only future research can confirm if it it could be generalized to the population of the Netherlands. There could also be a comparison with other countries, in Europe or world wide. Some countries have very strict privacy laws, where countries have surveillance on a big scale. This study creates a further avenue of research addressing embedded, less well-known ways of tracking users.

This study was conducted using literature research and models that where not yet studied in the context of this study before. In addition, the scales used in this study need to be further optimized, as some items could not be used due to lack of reliability or factorial validity.

Because the privacy calculus is never used before to investigate the privacy concerns of citizens of smart cities, it is therefore difficult to indicate if the privacy calculus is suitable enough to predict peoples attitude towards data disclosure in the form of Wi-Fi tracking. In this study, it was however not possible to validate the full model of the privacy calculus, although people with high concerns regarding their privacy, tend to have a negative attitude towards data disclosure. The possible Benefits and possible privacy concerns and risks where adopted from previous studies regarding the privacy calculus. Possible other risks and concerns are more applicable in the case of Wi-Fi tracking. This study is foremost a preliminary investigation, where future research can built on.

The privacy concerns of people living in smart environments is an interesting research topic. It already shows that people see the possible benefits of Wi-Fi tracking, but that there also are a lot of concerns. Future research can try to focus on, how these privacy concerns related to other privacy invasive technologies.

Future research can attempt to capture the awareness of citizens again, to see if the placement of the signs will make a differences in awareness and in the constructs of the privacy calculus (Trust, Risks, Concerns, Benefits and Willingness to disclose data. Furthermore, future research can focus on differences or similarities between different cities with regards to the awareness and privacy concerns.

In the open comments people stated that hacking is one of their concerns. Hacking is not further described in this research. Future research should investigate how big of a threat this could be. Also the ethical aspects of Wi-Fi tracking can be examined. Ethically, it makes sense that everybody knows what is happening to their data, how an entity is using it, how the provider can benefit from the data disclosure and what the possible consequences are.

## IX. LITERATURE


Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, *22*(1), 3-21.

Aleisa, N., & Renaud, K. (2017). Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions.

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. In *International Conference on Smart Cities, Infrastructure, Technologies and Applications* (pp. 123-138). Springer, Cham.

Asin and D. Gascon, "50 Sensor Applications for a Smarter World," 2012.

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

Barkhuus, L. and A.K. Dey, "Location-Basedservices formobiletelephony: astudyofusers'privacyconcerns.," inINTERACT. 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*.

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)

Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. Proceedings of the ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Montreal, PQ, Canada, 9–14 September 2007

Clarke, I (2001) Emerging value propositions for M-commerce. Journal of Business Strategies

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

Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1-9). IEEE.

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

Cunche, M. (2014). I know your MAC Address: Targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*, *10*(4), 219-227.

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.

Fife, E., & Orjuela, J. MOBILE PHONES AND USER PERCEPTIONS OF PRIVACY AND SECURITY.

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.

Gassen, M., & Fhom, H. S. (2016). Towards Privacy-preserving Mobile Location Analytics. In EDBT/ICDT Workshops.

Giusto, D. Iera, A. Morabito, G. and L. Atzori, Eds. Springer New York, 2010, pp. 389–395

Giffinger, R., & Gudrun, H. (2010). Smart cities ranking: an effective instrument for the positioning of the cities?. *ACE: Architecture, City and Environment*, *4*(12), 7-26.
Hancke, G. P., & Hancke Jr, G. P. (2012). The role of advanced sensing in smart cities. *Sensors*, *13*(1), 393-425.

Haas, M. C. (2016). Preserving Privacy by Detecting and Exploiting WiFi-scanners.

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).

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

Herrmann, M., Hildebrandt, M., Tielemans, L., & Diaz, C. (2016). Privacy in Location-Based Services: An Interdisciplinary Approach. *SCRIPTed*, *13*, 144.

Hochheiser, M. (2015). The Truth Behind Data Collection and Analysis, 32 J. Marshall J. Info. Tech. & Privacy L. 33 (2015). *The John Marshall Journal of Information Technology & Privacy Law*, *32*(1), 3.

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

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, *71*(12), 1163-1173.

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174-182.

Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security.

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. Inference Attacks on Location Tracks. Proceedings of the International Conference on Pervasive Computing (Pervasive), Toronto, ON, Canada, 13–16 May 2007; Voume 4480, pp. 127–143.

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

Levenbach, F. M. (2017). The smart city trade-off.

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.

C. M. Medaglia and A. Serbanati, “An overview of privacy and security issues in the Internet of Things,” The Internet of Things, .

Mena, J. (2013). Data mining mobile devices. CRC Press.

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.

Motiwalla, L.F., Li, X., Liu, X., 2014. Privacy paradox: Does stated privacy concerns translate into the valuation of personal information?. In: Proceeding of the 19th Pacific Asia Conference on Information Systems (PACIS 2014), Paper 281.

Mukhopadhyay, S. C., & Suryadevara, N. K. (2014). Internet of things: Challenges and opportunities. In *Internet of Things* (pp. 1-17). Springer International Publishing.

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.

Neirotti, Paolo, Alberto De Marco, Anna Corinna Cagliano, Giulio Mangano, and Francesco Scorrano. "Current trends in Smart City initiatives: Some stylised facts." *Cities* 38 (2014): 25-36.

Pang, J., Greenstein, B., Gummadi, R., Seshan, S., & Wetherall, D. (2007, September). 802.11 user fingerprinting. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking* (pp. 99-110). ACM.

Pan, G., Qi, G., Zhang, W., Li, S., Wu, Z., & Yang, L. T. (2013). Trace analysis and mining for smart cities: issues, methods, and applications. IEEE Communications Magazine, 51(6), 120-126.

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.

Schauer, L., Werner, M., & Marcus, P. (2014, December). Estimating crowd densities and pedestrian flows using wi-fi and bluetooth. In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 171-177). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Shin, M., Cornelius, C., Kapadia, A., Triandopoulos, N., & Kotz, D. (2015). Location privacy for mobile crowd sensing through population mapping. Sensors, 15(7), 15285-15310.

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.

Su, K., Li, J., & Fu, H. (2011, September). Smart city and the applications. In Electronics, Communications and Control (ICECC), 2011 International Conference on (pp. 1028-1031). IEEE.

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, xxvii.

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.

Want, R., & Dustdar, S. (2015). Activating the Internet of Things [Guest editors' introduction]. *Computer*, *48*(9), 16-20.

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.

Wilson, S. (2014). The collision between Big Data and privacy law. Browser Download This Paper.

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/ResearchInProgress/101

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

Youm, H. Y. (2017). An Overview of Security and Privacy Issues for Internet of Things. *IEICE TRANSACTIONS on Information and Systems*, *100*(8), 1649-1662.

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.

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). Sensing as a service and big data. arXiv preprint arXiv:1301.0159.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742.

## X. APPENDIX

A. Correlation matrix

**Correlations**

| | | | Risks | Concerns | Trust | Benefits | Attitude |
|---|---|---|---|---|---|---|---|
| Spearman's rho | Risks | Correlation Coefficient | 1,000 | ,496** | ,440** | ,454** | ,349** |
| | | Sig. (2-tailed) | . | ,000 | ,000 | ,000 | ,001 |
| | | N | 86 | 86 | 86 | 86 | 86 |
| | Concerns | Correlation Coefficient | ,496** | 1,000 | ,486** | ,497** | ,326** |
| | | Sig. (2-tailed) | ,000 | . | ,000 | ,000 | ,002 |
| | | N | 86 | 86 | 86 | 86 | 86 |
| | Trust | Correlation Coefficient | ,440** | ,486** | 1,000 | ,688** | ,623** |
| | | Sig. (2-tailed) | ,000 | ,000 | . | ,000 | ,000 |
| | | N | 86 | 86 | 86 | 86 | 86 |
| | Benefits | Correlation Coefficient | ,454** | ,497** | ,688** | 1,000 | ,620** |
| | | Sig. (2-tailed) | ,000 | ,000 | ,000 | . | ,000 |
| | | N | 86 | 86 | 86 | 86 | 86 |
| | Attitude | Correlation Coefficient | ,349** | ,326** | ,623** | ,620** | 1,000 |
| | | Sig. (2-tailed) | ,001 | ,002 | ,000 | ,000 | . |
| | | N | 86 | 86 | 86 | 86 | 86 |

**. Correlation is significant at the 0.01 level (2-tailed).

B. Regression coefficients

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. | 90,0% Confidence Interval for B | |
|---|---|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | | Lower Bound | Upper Bound |
| 1 | (Constant) | ,218 | ,396 | | ,552 | ,583 | -,569 | 1,006 |
| | Risks | ,125 | ,124 | ,099 | 1,005 | ,318 | -,122 | ,372 |
| | Concerns | -,059 | ,096 | -,062 | -,608 | ,545 | -,250 | ,133 |
| | Trust | ,373 | ,123 | ,357 | 3,043 | ,003 | ,129 | ,617 |
| | Personal interest | ,367 | ,119 | ,362 | 3,087 | ,003 | ,130 | ,603 |

a. Dependent Variable: latent_attitude

C. LITERATURE OVERVIEW

| **Authors:** | **Information:** |
|---|---|
| Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Atzori, L., Iera, A., & Morabito, G. (2010). | IOT & Smart cities |
| Dinev, T., & Hart, P. (2006). Barth, S., & de Jong, M. (2017). | Privacy calculus model |
| Demir, L., Cunche, M., & Lauradoux, C. (2014, June). Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Pan, G., Qi, G., Zhang, W., Li, S., Wu, Z., & Yang, L. T. (2013). | Purposes of Wi-Fi tracking |
| Finn, Wright and Friedewald, (2013) | Privacy of location |
| Gassen & Fhom (2016); Bailey, (2015) | Awareness of Wi-Fi tracking |
| Barth, S., & de Jong, M. (2017). | Privacy paradox |
| Malhotra, N. K., Kim, S. & Agarwal, J. (2004). Xu,Teo, Tan & Agarwal, (2009) | Privacy concerns |
| Dinev and Hart (2006) Malhotra, N. K., Kim, S. & Agarwal, J. (2004). Anderson and Agarwal (2011) Xu,Teo, Tan & Agarwal, 2009 | Survey constructs |
| Schauer, L., Werner, M., & Marcus, P. (2014, December) Cunche, M. (2014) | Wi-Fi tracking: Mac address |

C. Questionnaire

Study's instrument items.

All items employ 5-point Likert scale.
Example interview based on Dinev and Hart (2006). The actual items were slightly modified from the original instruments to capture the context of this study.

| | |
|---|---|
| Leeftijd: | |
| Geslacht: | |

Bedrijven en gemeenten maken soms gebruik van wifi-telling. Via wifi-tellingen worden locatiegegevens met het unieke nummer van je mobiele apparaat, zoals een tablet en smartphone, opgeslagen en verwerkt. Winkels kunnen deze informatie gebruiken om bij te houden hoeveel mensen langs de winkel lopen, de winkel binnenlopen en welke plekken zij in de winkel bezoeken. Gemeenten kunnen de techniek van wifi-telling inzetten om loopstromen van grote groepen mensen in kaart te brengen, bijvoorbeeld tijdens grote evenementen zoals Koningsdag en festivals. Deze informatie kan bijvoorbeeld worden gebruikt om te zien of het op een bepaalde plek in de stad té druk wordt en de mensenmassa moet worden omgeleid of om te bepalen waar extra hulpdiensten moeten worden ingezet. Via wifi-telling ben je dus te volgen door bedrijven en gemeenten.

Geef aan in hoeverre u het eens bent met de volgende stellingen. De antwoorden gaan van " totaal mee eens" naar " totaal mee oneens". Waarbij 3 neutraal is.

| **A** | **Awareness: In hoeverre bent u bekend met Wi-Fi telling** ***Totaal mee eens – Totaal mee oneens*** |
|---|---|
| A1 | Had u al eens eerder gehoord van Wi-Fi telling? JA/NEE |
| A2 | Ik weet dat gemeenten, waaronder Enschede Wifi tracking uitvoeren? JA/NEE |
| A3 | Ik weet dat gemeenten en winkels mij door middel van mijn telefoon kunnen volgen in de stad. |
| A4 | Ik ben me NIET bewust van het feit dat mijn data constant zou kunnen worden verzameld via mijn telefoon, wanneer ik door de stad loop. Totaal mee eens / totaal mee oneens |
| A5 | Ik ben me bewust dat Wi-Fi tellingen ook mogelijk zijn, zonder dat ik verbonden ben met een Wi-Fi netwerk. Totaal mee eens / totaal mee oneens |
| A6 | Ik weet voor welke doeleinden de gemeente Wi-Fi tellingen uitvoert. Totaal mee eens / totaal mee oneens |

De volgende vragen zijn gericht om te achterhalen In hoeverre is binnenstad monitoring (Wi-Fi tellingen) voor u persoonlijk interessant kan zijn.

| **B**Poikela, M., Wechsung, I., & Möller, S. (2015, July). Location-Based Applications-Benefits, Risks, and Concerns as Usage Predictors. In *Symposium on Usable Privacy and Security (SOUPS)*. | **Benefits / personal interest: In hoeverre is Wi-Fi tracking voor u persoonlijk relevant?** *Totaal mee eens – totaal mee oneens* |
|---|---|
| B1 | Wi-Fi tracking kan me de volgende voordelen bedieden.<br>Veiligheid<br>Gebruik van open Wi-Fi hotspots<br>Persoonlijke aanbiedingen<br>De leefbaarheid in de stad (voorzieningen)<br>Het in kaart brengen van bezoekersstromen<br>Nooit |
| B2 | Indien u bij de vorige vraag 'anders namelijk' had ingevuld, kunt u hieronder aangeven in welk geval u Wi-Fi tellingen acceptabel vind. |
| B3 | Ik ben van mening dat als gevolg van het verzamelen van mijn persoonlijke informatie, ik zal profiteren van een betere stad / services |
| B4 | De mogelijke voordelen die ik kan hebben van Wi-Fi tracking, zorgen ervoor dat ik geen of minder problemen heb met Wi-Fi tracking |
| B5 | Het verzamelen van data doormiddel van Wi-Fi telling is nuttig. |
| B6 | Het belang dat gemeenten hebben, bij het verzamelen en verwerken van persoonlijke gegevens, weegt minder zwaar dan de belangen van de personen van wie deze data afkomstig is. |

| **T**<br>**Adapted from Dinev & Hart (2004, 2006)**<br>**Malhotra et al. (2004)**<br>**Westin (2001)** | **Trust. In hoeverre gaan overheden en bedrijven vertrouwelijk om met mijn informatie.**<br>*Totaal mee eens – totaal mee oneens* |
|---|---|
| T1 | Ik vertrouw erop dat gemeenten / overheid mijn persoonlijke gegevens niet onjuist zullen gebruiken. |
| T2 | De meeste organisaties en overheden verwerken de persoonlijke informatie die zij over mensen verzamelen op een juiste en vertrouwelijke manier |
| T3 | De meeste organisaties en overheden hebben een goede ethiek en motivatie met betrekking tot het omgaan met de persoonlijke informatie van mensen |
| T4 | Bestaande wetten en organisatiepraktijken bieden tegenwoordig een redelijk niveau van bescherming voor de privacy van burgers. |

Geef aan in welke mate u denk dat de risico's aanwezig zijn. Antwoorden gaan van "erg klein risico" tot "erg groot risico" waarbij 3 neutraal is.

| **PR.**<br>**Adapted from Dinev & Hart (2004, 2006)** | **Privacy risks: Hoeveel risico verwacht u dat er is wanneer er Wi-Fi tracking plaats vind in uw stad.** *Erg klein risico– erg groot risico* |
|---|---|
| PR1 | Persoonlijke gegevens die zijn verzameld, kunnen worden misbruikt. |
| PR2 | Persoonlijke informatie kan zonder mijn medeweten beschikbaar worden gesteld aan anderen. |
| PR3 | Persoonlijke informatie kan op ongepaste wijze worden gebruikt |
| PR4 | Er is een grote kans op het verlies van privacy wanneer gemeenten Wi-Fi tellingen uitvoeren |

| **PC. Adapted from Dinev & Hart (2004, 2006); Malhotra et al** | **Privacy concerns (PC) In hoeverre denkt u dat uw privacy in het geding is, door de Wi-Fi tracking door gemeenten en winkels?** *Totaal mee eens – totaal mee oneens* |
|---|---|
| PC1 | Heeft u zorgen over het feit dat gemeenten Wi-Fi telling uitvoeren? Zo ja, wat zijn deze zorgen? |
| PC2 | Ik maak me zorgen dat de informatie die verzameld wordt, kan worden misbruikt. |
| PC3 | Ik maak me zorgen over het verzamelen van mijn informatie met Wi-Fi tracking, vanwege wat anderen met mijn informatie zouden kunnen doen. |
| PC4 | Ik maak me zorgen over het verzamelen van mijn persoonlijke informatie, omdat het kan worden gebruikt op een manier die ik niet had voorzien. |
| PC5 | Ik maak me zorgen de controle te verliezen over hoe persoonlijke informatie wordt verzameld en gebruikt door gemeenten |

| **ATT** | Attitude: |
|---|---|
| ATT1<br>**Adapted from Anderson and Agarwal (2011)**<br><br>*Totaal mee eens – totaal mee oneens* | Ik ben bereid mee te werken, wanneer mijn gemeente mij mededeelt dat ze Wi-Fi telling willen uitvoeren. |
| ATT2 | Het is waarschijnlijk dat ik zou mee werken, wanneer mijn gemeente mij mededeelt dat ze Wi-Fi telling willen uitvoeren. |
| ATT3 | Het maakt mij niks uit of gemeenten Wi-Fi tracking uitvoeren |
| | Wi-Fi telling gebeurd automatisch wanneer je je in de binnenstad begeeft. Bij het opt-out systeem word je telefoon automatisch gevolgd. Wanneer je dit niet wilt, zal je je hiervoor moeten uitschrijven (zogenoemd opt-out) Dit is mogelijk op de website van het bedrijf dat de Wi-Fi telling uitvoert. |
| ATT4 | Ik zou overwegen om de zogeheten opt-out (aangeven dat u bezwaar hebt en niet wilt worden gevolgd) optie te gebruiken, zodat mijn wifi niet meer wordt gemonitord. |
| ATT5 | Wanneer ik me bewust ben en kennis heb van hoe mijn data word verzameld en gebruikt, heb ik minder problemen met Wi-Fi tellingen die worden uitgevoerd. |