PRIVACY PROTECTION IN DUTCH SMART CITY INITIATIVES

A research on the consideration for privacy implications by policy makers

Boris van den Berg S1425595

Master Crisis and Security Management

Leiden University

Supervisor: Dr.ir. V. Niculescu-Dinca

Second reader: Dr. T. van Steen

Word count: 19,242 (Excluding references, footnotes, contents, abstract)

Date: 21-02-2020

Abstract

The increasing world population and urbanization are causing challenges for the cities of the future. To face these challenges, many cities are looking into ICT solutions to become more efficient and to be able to provide better services to the public. Smart cities can be the solution to the rising challenges, providing the ability monitor, manage and regulate by continuous computing and digitally instrumented devices that are integrated into the urban environment. The downside of smart cities is that they can cause privacy threats to the public. This research has investigated the consideration of privacy implications of smart city initiatives. This research has been done by conducting expert interviews with project managers from four different smart city initiatives in multiple cities of The Netherlands. The data collected from the interviews is thereafter crossed with theories on privacy protection in smart cities and privacy protection frameworks to conclude. The results from this research indicate that the four smart city initiatives are actively taking measures to prevent privacy threats from occurring and work with Privacy by Design principles and the data regulation policies, which means the initiatives take privacy implications of their operations into account. There are still some privacy implications not completely considered and addressed by the initiatives, resulting in some privacy threats. These privacy threats are caused by a lack of legal clarity of data ownership and not adequately addressing the importance of the role of individuals in privacy protection.

Acknowledgements

I would first like to thank my supervisor Dr.ir. V. Niculescu-Dinca for his input and advice to help shape this research. Being able to use his network for data collection has been essential for this research. I would also like to thank my second reader Dr. T. van Steen for his comments and feedback on multiple occasions.

Lastly, I would like to thank the experts that have participated in the interview sessions: The project manager of Burgerparticipatiesysteem Leefbaarheid & Veiligheid, project manager of Inbraakvrije Wijk Guido Delver, project manager of City Lab Eindhoven Tinus Kanters and project manager of Digital Perimeter Daan Groenink. Without their participation and openness, this research would not have been completed.

Contents

Introduction

According to the UN, by the year of 2100 the world population is predicted to have reached over 11.2 billion people, an increase which is considered a 'medium growth'. The expected growth is equivalent to seven times the population of the European Union countries, and will require the upscaling of infrastructure, development and will lead to more pressure on material resources.[1] The population increase is almost inevitable, even though fertility rates have declined since the 1970s. But if the fertility rates somehow stop declining the estimated world population would be around 16.6 billion people, 5 billion more than the current estimate.[2] Besides the increasing world population, urbanization is also an issue that will have to be dealt with in the near future. Nowadays, more than half of the world's population live in urban areas. The trend of people moving from rural areas to urban areas will continue in the coming decades, because of a lack of resources in rural areas and the believe that the standard of living is better in cities. Practically all the population growth estimated for the 21st century will occur in the poorest countries on the globe which will result in increases in pollution and epidemics (due to their lack of resources to manage these problems). Expectations are that by the year 2050 the total amount of people living in urban areas will surpass the current world population. In 1950, New York and London were the only two cities in the world that had a population of more than 10 million inhabitants.[3] In 2016, according to a UN report, 31 megacities across the world accommodate more than 10 million inhabitants,[4] illustrating the increasing world population and urbanization of the last 70 years. The increasing world population and urbanization are presenting new challenges to cities and communities. Cities will become chaotic and disorganized due to the increase in population if these upcoming issues are not dealt with properly (Chourabi, Nam, Walker, Gil-Garcia, Mellouli, Nahon & Scholl, 2012: 2289). Cities will have to find new solution to be able to accommodate the increasing number of residents. To be able to withstand the expansion of the civilian population, economic pressure, energy

[1] Smith, S. (2018, March 11). 'Two billion homes needed over next 80 years, studies show'. Accessed on https://www.independent.co.uk/life-style/design/housing-crisis-global-population-increase-two-billion-new-homes-80-years-end-of-century-a8245906.html

[2] Jones, S. & Anderson, M. (2015, July 29). 'Global population set to hit 9.7 billion people by 2050 despite fall in fertility'. Accessed on https://www.theguardian.com/global-development/2015/jul/29/un-world-population-prospects-the-2015-revision-9-7-billion-2050-fertility

[3] Mirkin, B. (2014, April 3). 'World Population Trends Signal Dangers Ahead'. Accessed on https://yaleglobal.yale.edu/content/world-population-trends-signal-dangers-ahead

[4] UN. (2014). 'The world's cities in 2016' Accessed on https://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf

consumption and environmental degradation, cities and communities are looking into information and communication technology (ICT) solutions. Due to the possibility of ICT solutions the interest in smart cities has increased over the last years. Smart cities are cities that embrace ICT as a development strategy. These cities embed digital systems and infrastructures into their urban fabric and use them for regulatory and entrepreneurial purposes (Kitchin, 2014: 1). The cities and communities are aiming to use ICT services and other smart solutions to develop a smart city, able to withstand the problems of the future. Smart cities are attractive because they are designed with the goal to provide better services with lower costs through ICT solutions and trends (Mohamed, Idries, Mohamed, Al-Jaroodi & Jawhar, 2014: 267).

Research question

The increasing use of ICT systems by cities is opening a new world of possibilities, but also invites new risks. When more information is collected by city ICT systems, more information is available to hackers and other threats. This research will investigate emerging smart city initiatives in The Netherlands with a focus on how the consideration for civilian privacy is included in the making and execution of these initiatives. Important here is that policy makers work for civilians, therefore these civilians should be protected and respected during the making of future smart city plans. This leads to the research question of this research: *To what extent are privacy implications taken into consideration by policy makers with the implementation of smart city initiatives in The Netherlands?*

This research focusses on smart city initiatives in the five biggest municipalities in the Netherlands. These municipalities work together by exchanging information on new smart city initiatives and technologies. The Hague for example was assigned the topic Safety and Security,[5] a topic closely related with this research because it looks at the privacy and safety of civilians in smart cities. However, this does not exclude the other cities who might have different initiatives because this would limit the scope of this research and therefore decrease the chance of generalization possibilities.

Relevance

Smart cities are only a recent trend and are still a work in progress, so the research on the privacy risks of smart cities and the performance of smart cities with privacy protection is still

[5] VNG. (2018, August 13). 'Smart City Den Haag zet stappen'. Accessed on https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/smart-society/nieuws/smart-city-den-haag-zet-stappen

limited. Smart city initiatives do contain some privacy and public safety risks if left unchecked and therefore require more intensive political, legal and scientific attention. Cybercrime is one of the biggest threats for achieving reliable and favorable smart cities. These challenges need continuous attention and cooperation from all stakeholders like the government, legal institutions, politicians, the industries, research laboratories and network operators (Khatoun & Zeadally, 2017: 58). Exploring the new problems and possible solutions with regards to the topic of smart cities will not only help shape the dialogue but can also guide future researchers towards new insights. In addition to this privacy in smart cities does differ from the traditional concept of privacy thus increasing scientific relevance of this research. The legal privacy frameworks created in the nineteenth and twentieth century are not capable of assessing the privacy concerns in a smart urban public space. With the introduction of the General Data Protection Regulation and Privacy by Design (from now on GDPR and PbD, will be discussed in the theoretical framework), new frameworks for privacy protection have been introduced. It is thus important to investigate new frameworks and their ability to address the challenge of preserving privacy. (Koops, Newell & Skorvánek, 2018: 78). The content of the GDPR and PbD will be explained in the theoretical framework. To my knowledge, there has not been a research on privacy protection while focussing directly on a smart city project, which means this research is one of the first to evaluate privacy protection on the street level.

The social relevance of this research is the fact that new insights on the privacy risks of smart city initiatives for civilians can help smart cities to protect them more effectively against hackers and other perpetrators. Eckhoff and Wagner (2017: 21) believe that the awareness of privacy risks that come with the technologies and applications of smart cities needs to be improved. They state that it is important that people understand that there is value attached to personal data. Eckhoff and Wagner see the increasing of privacy awareness as a big challenge, because it is not in the hands of researchers, but in the hands of political powers and the media. After an analysis of smart cities around the world, the results were that a big number of the smart cities had insufficient privacy protection and information on privacy policies (Eckhoff & Wagner, 2017: 21). A study by Ståhlbröst, Padyab, Sällström & Hollosi (2015: 11) showed that citizens are concerned that their data that is collected for a certain purpose, might be used for other purposes while it is still available. Providing more clarity on what smart cities do to protect the citizens privacy will take away the concerns when the privacy protection is satisfactory or will put pressure on the smart cities to improve their privacy protection if it is unsatisfactory. On the other hand, if smart city projects in The Netherlands turn out to be exceptional in privacy

protection, it could serve as an example for other cities trying to become smarter. Privacy is one of the main concerns when thinking about the dangers of smart cities, so if smart cities can show that they can protect people their privacy, while being better able to offer good services to the public than regular cities, more people will be open to the idea of smart cities. Citizens need to feel secure and confident enough to engage with the smart city, because that is needed for the smart city to provide better quality of urban life and to become more efficient. If the citizens are not interested in the smart city, because of inadequate security and privacy protection, the smart city will never be a success (Braun et al., 2018: 2-3). Smart cities are one of the solutions for the urbanization and growing world population but need to get rid of the privacy concerns to get citizens to participate. If there is more room for the construction of smart cities, a better-quality life can be provided to the masses (Braun, Fung, Iqbal & Shah, 2018: 1).

Theoretical framework

In this chapter, a literature review will be done on smart cities and the privacy risks they pose to society. At first, more information on smart cities and a definition will be displayed. Thereafter, the causes of the upcoming of smart cities will be explained. This will be followed by the conceptualization of privacy to be able to make a distinction between multiple privacy types. This distinction can be used to determine the risks of smart cities regarding privacy of civilians. This literature review leads to the finding of a research gap which this research is attempting to fill. Furthermore, frameworks for the evaluation of privacy protection will be explained, to create the ability to evaluate the case study of a smart city project later in the research. The theoretical framework will end with an explanation of the conceptual model.

What is a smart city?

The smart city can be a complicated subject because it has not been possible to come to a single comprehensive definition, so it is important to elaborate on what a smart city is and present a definition from the literature that will be used in this research. Smart cities are not so new as one may think, traces of plans related to smart cities can be traced back to the late 1990s with the Smart Growth Movement. If one would dig deeper, they would find that even in the 1960s there were plans of 'cybernetically planned cities', which can be linked to the concept of the smart city (Höjer & Wangel, 2015: 337).

Kitchin (2013: 1-2) has two views on what a smart city is. His first view on what a smart city is, can be explained as an urban place being extensively monitored, managed and regulated by continuous computing and digitally instrumented devices that are integrated into the urban environment. This approach is characterized by digitally controlled utility services and transport infrastructure as well as installation of sensors and camera systems connected to wireless telecom networks. Smartphones of citizens are being used to collect data on their location and activities, while the citizens on the other hand use their smartphone to engage with smart city features. This way the smart city can often in real-time monitor and manage the city's circumstances (Kitchin, 2013: 1-2). The second view on smart cities refers more to the improving of the knowledge economy within the region of a city. This perspective sees smart cities as being driven by entrepreneurship, creativity and innovation. To achieve these ideas and innovations in relation to professional services the concept of ICT is the central and most important factor to achieve these goals. However, it is important to note that the use of ICT does not mean a city is smart; ICT must work together with economic policies and human

capital in order to facilitate in urban improvements (Kitchin, 2013: 2). These two perspectives are united by the neoliberal ideology that focuses on governance of urban areas through technological and market-led approaches. The biggest promoters of the development of smart cities are big businesses that want to push the government to adopt their newly developed technologies and try to achieve a more privatized, deregulated and open economy (Kitchin, 2013: 2).

As mentioned, the use of smart cities is mainly promoted by the private sector, ICT and infrastructure companies. Although many of the technologies used in smart city initiatives already exist it is the use of synchronization and interconnection between these systems/technologies that make smart cities innovative. The challenges of smart cities can mostly be found in the interconnectivity and is thus interesting for companies that are able to come with useful solutions (Höjer & Wangel, 2015: 337). There is a risk that public policies are being ignored to follow market imperatives, because corporate businesses push local governments to adopt their technologies and applications, which creates problems for the local governments (Van Zoonen, 2016: 473). For city, national and supra-national governments, smart cities are appealing because of their potential to make cities more secure, liveable, sustainable and competitive (Kitchin, 2013: 2).

It is important to get to a single definition of the concept of smart cities before further research. In this research, the following definition of the concept smart city will be used:

> "The use of Smart Computing technologies to make the critical infrastructure components and services of a city—which include city administration, education, healthcare, public safety, real estate, transportation, and utilities—more intelligent, interconnected, and efficient" (Chourabi et al., 2012: 2290).

The central aim of a smart city is thus to offer services to civilians at a lower price due to costs effective management while at the same time creating a more efficient infrastructure. This should make the city more sustainable and attractive to the public. To achieve this goal, the smart city seeks to use ICT trends and solutions, such as new technology applications and the internet of things (IoT) (Mohammed et al., 2014: 267).

Why are smart cities needed?

This chapter will provide different challenges cities around the world could face in the future leading to a higher demand for smart solutions. Firstly, the world population is rapidly

increasing, together with the trend of people moving to the cities in greater amounts. Secondly, economic growth causes that more areas are required to be occupied by civilians. Thirdly, cities need to become more sustainable and control their emissions because of environmental requirements and if they keep growing, these challenges will become harder to overcome. Lastly, because of the global economic instability, cities are forced to become more independent and sustainable (Mohammed et al., 2014: 269). These challenges are not completely related to each other but are different situations cities can face that ask for smart city solutions.

In order to handle the rising global population many cities must adapt their physical infrastructure to cope with the rise in population. Adapting to the rise of people living in cities is important because left unchecked it would result in unfavorable living conditions because cities will not be able to provide proper security, effective and efficient healthcare and education towards citizens now living in these cities. If no serious measures are being taken by those cities, increased cyberattack threats, environmental degradation and poverty are possible outcomes. Rethinking access to transport, energy management, waste management and other resources is essential for the challenged cities (Khatoun & Zeadally, 2017: 51).

Conceptualizing privacy

Smart cities have their advantages, but because they rely heavily on technologies, one of the main problems is how they are going to ensure good privacy protection for the citizens. Before the privacy issues in smart cities will be further elaborated, a conceptualization of privacy will be given to guide this research.

Although a widely accepted definition of privacy does not yet exist, even though many researchers have tried to conceptualize it, there is a growing consensus amongst researchers that privacy does consist of multiple dimensions (Finn, Wright & Friedewald, 2013: 6). Because there is no widely accepted definition, this research will use the definition of Finn, Wright and Friedewald, who based their seven types of privacy on the 4 categories of privacy outlined by Roger Clarke in 1997. It is important to define privacy, because there are multiple views on privacy, as there is still no widely accepted definition. This definition of privacy will help this research with analysing privacy protection and determine what types of privacy are protected and what not.

The first type of privacy is **privacy of the person**, also named as bodily privacy. This right calls for the protection of the integrity of the physical person (Kitchin, 2016: 5). Privacy of the person is the right to keep characteristics and functions of the body private. Examples are

genetic codes and biometrics like DNA and fingerprints. Privacy of the person is believed to create individual feelings of freedom and providing it to the people will support a healthy democratic society (Finn, Wright & Friedewald, 2013: 8).

The second type of privacy is **privacy of behaviour and action**. This type of privacy contains sensitive topics as religious practices, political activities, habits and sexual preferences. It means that individuals should be free to exhibit their behaviour and actions in either public or private spaces without being monitored or controlled. This would contribute to the freedom and autonomy in thought and action of individuals (Finn, Wright & Friedewald, 2013: 8).

Privacy of communication is the next type of privacy, which aims at avoiding communications being intercepted. Civilians conversations and correspondence are protected from surveillance because of communications privacy (Kitchin, 2016: 5). This includes the interception of emails, the use of directional microphones, intercepting phone calls or other wireless communication. Privacy of communication is recognised by many governments, which is the reason that wiretapping and other ways to intercept communications always needs to be overseen by a judicial authority. The right of privacy provides benefits towards individuals and society because it enables and encourages them to partake in free discussions surrounding a wide range of topics while it also stimulates growth in the communications sector (Finn, Wright & Friedewald, 2013: 8).

The following type of privacy is **privacy of data and image**, which is involved with making sure that the data of individuals is not automatically available to others and that individuals have some control over their data and the use of it. If individuals have control over their data, they are enabled to feel empowered and build self-confidence. Privacy of data and image addresses the balance of power between the individual and the state, which gives this type of privacy social value (Finn, Wright & Friedewald, 2013: 8). This type of privacy is especially important in this research because data protection is one of the bigger issues facing smart city initiatives.

The fifth type is **privacy of thoughts and feelings**. This type gives individuals the right to share or not share their feelings or thoughts and the right to think whatever the individual would like. This right gives the individual freedom and power relative to the state. This type of privacy can be distinguished from the right to privacy of the person and behaviour, because the mind and the body are different from each other and thoughts do not automatically turn into actions (Finn, Wright & Friedewald, 2013: 9).

The following type described in the article of Finn, Wright and Friedewald is **privacy of location and space**. Civilians are often protected against the tracking of their spatial behaviour (Kitchin, 2016: 5). This would give individuals the right to be able to move around public and semi-public space without being monitored, tracked or identified. This also includes the right to privacy in individual's homes, cars and workplaces. Being able to move around without the fear of being monitored gives individuals the experience of freedom which is one of the core values of living in a democracy. Freedom of assembly and dissent is encouraged because of the privacy of location and space, which are important elements for a healthy democracy (Finn, Wright & Friedewald, 2013: 9)

The seventh and last type of privacy that was identified by the article is **privacy of association**. This gives people the right to associate with whomever they want to, without being monitored. This right promotes freedom of association, freedom of worship and freedom of speech, which are essential for democratic societies. Marginalised voices, which can press for economic or political changes, have more chance of being heard when they are able to associate with each other (Finn, Wright & Friedewald, 2013: 9).

Technologies used in smart cities, mostly driven by data collection create multiple possible privacy risks and create big challenges for the existing way of thinking about the protection of privacy (Kitchin, 2016: 5). All the privacy types mentioned above can be violated if smart cities do not take the privacy implications of their projects and technologies into consideration.

Privacy issues in smart cities

The concept of privacy has been conceptualized in seven different types, which allows us to not only have a better look at the privacy issues that can occur in smart cities, but it also enables us to link these issues to privacy conceptions. According to Zhang, Ni, Yang, Liang, Ren and Shen (2017: 125), smart cities should be able to protect information they collect from disclosure, modification, disruption, inspection, annihilation and unauthorised access. To achieve this, smart cities need to fulfil privacy and security requirements such as integrity, confidentiality, access control, availability and privacy not only in the world of communication, but also in the information and physical world. Smart cities collect personal and sensitive information from the lives and environments of civilians and processes this information to impact the lives of the population. Collection and processing of personal information in order to impact the lives of civilians is not very popular among the general public and prevents smart cities from being attractive enough to inspire more use of their technologies (Zhang et al., 2017: 125). The

increase in data collection and processing by corporate systems increases the need for the balancing of data collection benefits with the rights of the individual. Urban life is increasingly being monitored, so to maintain the trust in the government and democracy, the usage of data needs to be overseen and abuse of data needs to be punished. Otherwise, a serious resistance against real-time analytics can grow among the citizens (Kitchin, 2013: 12). Smart cities need to work together with citizens to sustain the smart city's development, so they need to acknowledge the concerns of the people about their privacy, or smart city projects can become disputed and even cancelled (Van Zoonen, 2016: 472). One of the challenges for smart cities is that they need to develop policies that not only accommodate privacy concerns but are also more extensive than the minimal legal requirements. When developing smart city innovations or technologies, citizens are often neglected as partners. Their support and input are important, because citizens will be confronted with the smart city technologies and innovations in their daily lives (Van Zoonen, 2016: 479).

Before delving deeper into the challenges smart cities create, it is important to state that many of these challenges already exist. The problem is that the interconnectivity smart cities provide will cause more of these challenges to surface and become more frequent (Braun et al., 2018: 3). With the introduction of new technologies, guaranteeing the rights of citizens should always be a priority (Khatoun & Zeadally, 2017: 57). According to Khatoun and Zeadally (2017: 57), there are multiple benefits of the services a smart city can provide, but the invasion of privacy caused by smart city initiatives are becoming worrisome. Many smart city services depend on ICT, which means that users who are not familiar with technology and their security issues become easy targets for perpetrators. When people interact with smart city services through computers, smartphones or other devices, they reveal personal data such as their location, age and gender, which means they give up their privacy of data and image, privacy of location and space, and when the location on multiple moments in time is monitored, privacy of behaviour and action can also be ignored. An example to further explain the privacy challenges is the ownership of a car. The license plate of a vehicle can be connected to the owner and the movement of the car can easily be traced, endangering the privacy of location and space. Future vehicles in smart cities have multiple communication features, such as internet accessibility and GPS, which means that these vehicles can store personal information due to these online communication features. Because there will be a lot of similarly connected devices in a smart city, a lot of information is available for data consumers, including highly personal information like daily habits, which will endanger the privacy of behaviour and actions (Khatoun &

Zeadally, 2017: 57). The data on the location of an individual can reveal a lot about someone's life they do not want to share with the world. The connectivity of GPS systems can track the route taken together with the point of origin and destination. If a civilian set their GPS from their home, access to their locational data can reveal their home location. If the vehicle is away from home, their house is an easier target for criminal activities like burglary. If outside attackers can get access to people's contact lists and messages, they can use and reveal private matters that need to be kept personal for professional or commercial reasons, resulting in the violation of privacy of communications (Elmaghraby & Losavio, 2014: 494). Smart cities are created with the goal of improving services to the public to be able to give them a better-quality life, but the challenge is ensuring the privacy and security of the civilians (Khatoun & Zeadally, 2017: 57).

As mentioned earlier, it has become almost impossible to live in a smart city without leaving traces we create ourselves and traces that have been captured about us. According to Kitchin (2016: 7), it has now become easier to track the movement of individuals, because geo-location tracking is now able to monitor the location of individuals automatically, continuously, pervasive and relatively cheap. Geo-location tracking is a threat to the privacy of location and space, and as individuals can be tracked continuously, their actions and behaviours can also be analysed. In many cities, CCTV cameras are installed that can zoom in on individuals and track them. Machine vision algorithms can identify individuals trough TV facial recognition programmes, endangering the privacy of the person. The movement of cars is also registered, with ANPR cameras in the UK capturing 30 million plates every day with 8300 cameras (Kitchin, 2016: 7). Several cities have installed sensor networks, to track phones of pedestrians walking in the area. The data that was measured consisted of the speed of the individual, the proximity, the stores the individual visited, the amount of time they spent in the stores, and how often they visited the same stores. In combination with the CCTV cameras, it was possible to link the data of the sensors with the camera footage to collect data like the gender and age of the individual. These examples show that a lot of data on spatial behaviour is collected and processed. These data are often shared with other parties for governance or commercial purposes. Individuals are thus becoming more vulnerable to profiling and social sorting through geo-surveillance (Kitchin, 2016: 7-8). These new developments and technologies have major impacts on the privacy of location and space of individuals, behaviour and action and privacy of data and image, because the privacy of individuals is violated and the data that is collected is used for profiling and social sorting.

Anonymization of data is used to ensure the privacy for individuals when collecting data. The anonymization is done by using pseudonyms, aggregation or other techniques. This way, the individual's privacy is protected, because their personal data is not connected to the data in the database. The problem with anonymization is that it is often not very complicated to re-identify the data with the help of big data generation and computational technologies. Individuals in datasets get codes that are persistent and distinguishable, so it can be tracked over time to be able to create accurate individual profiles (Kitchin, 2016: 8). When data is deanonymized by other parties, the data will no longer be under control of the data subject, which means a violation of the privacy of data and image. In addition, the identity of the data subject is being revealed, violating the privacy of the person.

Because personal information in a smart city is gathered, spread and processed, there is a vulnerability to unauthorized access by outsiders and the leakage of privacy. The personal information smart cities use consists of the identity of the user, their location, the condition of their health and lifestyle. It would be a major failure, and violations of the privacy of the person, location and space, behaviour and action and data and image if this information would be leaked or traded to unauthorized parties (Zhang, Ni, Yang, Liang, Ren & Shen, 2017: 125). The reason data and data services are being traded is because it has formed into a multi-billion-dollar industry. In the US alone, 212 data brokers operate in the data sharing market together with 58 companies are in the business of tracking mobile locations. These data markets are the places data derived from the technologies and apps of smart cities will circulate (Kitchin, 2016: 10).

Individuals interact daily with smart city technologies, and these interactions happen very often and in diverse ways. This makes it hard for individuals to be in control of their privacy across all the smart city technologies and to make cost/benefit analyses of whether they agree with the terms and conditions of those technologies. Individuals need to give their consent before smart city technologies can collect and use their data, but this means that they are giving away their privacy without fully understanding the consequences of their actions. In a lot of cases, the notice of data collection and asking for consent is absent. Individuals are in these cases unaware of data being collected about them, so it is impossible to uncover the purposes for the collection of their data (Kitchin, 2016: 9). The individuals are thus not in control of their data, so their right to privacy of data and image is endangered.

Other issues of smart cities

Braun et al., (2018) have identified five challenges that smart cities will face. These challenges are relevant for this research because they give indications where and how privacy threats can occur. Organizations need to keep these challenges in mind when collecting, processing and sharing data in a smart city, because if these challenges are not properly taken care of, privacy issues will occur.

The first challenge is related to the interconnectivity of smart cities. The interconnectivity of smart cities implies that multiple parties can gain access to information, and these parties communicate that information with each other. Each organization that contributes to the smart city by sharing and processing information have their own way of dealing with the data. All these different ways of dealing with information can lead to personal privacy risks. The organizations contributing to the smart city will have diverse priorities, such as the difference in priorities between public and private actors. Private organizations will make a risk/profit analysis to decide to what extent of privacy protection is needed for their customers and will be rewarded for successful privacy protection, while public actors will likely be more intrinsically determined to achieve privacy protection, but are not dependent on the success of their privacy protection (Braun et al., 2018: 4-5). This illustrates the difference in approaches to privacy protection for private and public actors.

Secondly, a lot of individual smart devices are connected in a smart city, and their connection is relied upon. Providing protection for a single smart object like a smartphone or a website is much less complicated than the security of a city where all these objects are connected. This increases the attack surface for potential hackers. Every IoT device needs security, and because a smart city connects many devices, guaranteeing the security becomes a significant challenge. According to Mehmood, Ahmad, Yaqoob, Adnane, Imran and Guizani (2017: 21), around 70 percent of devices connected to the internet in a smart city are targets for cyberattacks because of weak encryptions, lacing software protection and insufficient authorization, according to HP. The vulnerabilities create multiple threats which lead to security and privacy issues (Mehmood, Ahmad, Yaqoob, Adnane, Imran & Guizani, 2017: 21). When an individual object is not adequately protected, the smart network can be accessed by hackers to gather information about the security circumstances of organizations that operate within the smart city (Braun et al., 2018: 7-8).

The third challenge for smart cities identified by Braun et al. (2018) is the enormous amount of data a smart city collects and processes, that need to be stored. Smart cities will use cloud services to store their data, because a smart city cannot save the data on physical drives, due to limited memory and computing power. When smart cities send their data to providers of cloud services, more potential data breach points are added. The cloud service providers have their own standards of privacy and security, which complicates the matter for smart cities. Furthermore, adding a third party like cloud service providers, questions about consent and responsibility arise. These third parties have the task to handle large amounts of private information, for which the data subjects may not have given their consent (Braun et al., 2018: 12). It remains unclear how trustworthy cloud service providers can be and if these providers cannot guarantee that the data is not used for anything other than just storing the data, privacy of data and image and possibly multiple other types of privacy can be violated.

The fourth challenge smart cities will face is secondary use of personal data. For example, when an individual applies for healthcare, they consent to sharing their personal information with the healthcare provider and the healthcare provider can process this information. The individual does not give consent for the healthcare provider to share their information with third parties and make money from it. When an individual's information is used in a manner which it was not intended for, it is not very clear whether their privacy is being violated. There are multiple private companies nowadays that earn money by sharing their collected data, but these companies can be avoided because they are not crucial part of daily life. If a private company is to perform an important smart city task, this company's presence has become unavoidable within the smart city. Fundamental organizations should thus be monitored on whether they use personal information for secondary purposes (Braun et al., 2018: 14). The secondary use of personal data makes it very difficult to know how the data is used and how it is transformed into new derived data. Kitchin (2016: 9) stated that data can be leaked, disclosed, intercepted, repurposed or disassembled across data streams. It is thus hard to track your data, see what happens to it and know who is handling your data. This makes it hard to hold data controllers accountable for their actions (Kitchin, 2016: 9). As with the third challenge, if there are no clear rules for the secondary use of data to ensure that data cannot be leaked or unjustly obtained, privacy of data and image and many other privacy types can be violated.

The last identified challenge is dealing with the cyberthreats that can pose serious threats to physical security (Braun et al., 2018: 16). Because this challenge concerning physical security is not linked to privacy threats, it will not be elaborated. What can be learned from this

challenge is that a good cybersecurity is not only vital to the protection of privacy, but also to physical security.

Research gap

The theories mentioned earlier show that there is a lot of knowledge on the privacy challenges surrounding smart cities. However, to my knowledge there has not yet been an evaluation of privacy protection policies in smart cities or smart city projects, which presents the opportunity to analyse the performance of smart cities in relation to privacy protection. This seems to be a gap in the academic knowledge on privacy protection in smart cities, a gap which this research is attempting to fill.

Frameworks for privacy protection

To be able to properly evaluate privacy protection policies in this research, three privacy frameworks are added to the theoretical framework. The first framework is contextual integrity, the second is Privacy by Design and the last is the General Data Protection Regulation, a legal framework developed by the EU. These three frameworks will be explained below.

Contextual integrity

Contextual integrity is a normative model or framework, created to evaluate information flows between agents to determine why some information flows create privacy issues and why others do not. Contextual integrity is normative because it emphasizes on explaining for what reason certain patterns of information flows cause public outcry regarding privacy violations. There are four key constructs when trying to define contextual integrity. These constructs are informational norms, appropriateness, roles and principles of transmission (Barth, Datta, Mitchell & Nissenbaum, 2006: 6). Before explaining the framework of contextual integrity, the concept of context should be further explored. Individuals do not act in an undifferentiated social world, but in certain roles or capacities in unique social contexts, like education (schools), healthcare (hospitals) and employment (job interviews). These different contexts are structured settings that have been evolving because of historical events, culture or location. The features of these contexts make up the roles individuals play and the norms for behaviour that lead to practices and actions (Barth, Datta, Mitchell & Nissenbaum, 2006: 2-3). The norms for behaviour and the roles of individuals can thus be different contexts.

The first construct needed to define contextual integrity is informational norms. Informational norms are rules that apply to the communication or transmission of personal data from one party

to another. An example of informational norms are the norms doctors must adhere to when talking about the health conditions of their patients to other people. Informational norms limit the amount of information that can be spread about a certain individual and can differ in different contexts. If these informational norms are breached in an unjust way, there is a violation of contextual integrity (Barth, Datta, Mitchell & Nissenbaum, 2006: 3).

The next construct for contextual integrity is appropriateness. Appropriateness creates a way to determine whether the information requested matches the relevant informational norms. A situation to illustrate appropriateness is a job interview. When the interviewer asks information on the marital status of the applicant, this is not relevant and inappropriate, but requesting information about the marital status of the applicant is appropriate when it is a dating site which requested the information. Appropriateness is a construct on its own and different from informational norms because the type of information influences the judgement of people (Barth, Datta, Mitchell & Nissenbaum, 2006: 3).

Roles are also a construct of contextual integrity. With every communication, three entities are relevant. These are the one sending information, the one receiving information and the information subject, whom the information is about. These three entities all behave in certain roles, which are associated with privileges and duties. When looking at whether a violation of contextual integrity has occurred, the roles of entities must be considered because they are key variables (Barth, Datta, Mitchell & Nissenbaum, 2006: 3).

Principles of transmission is the most distinctive construct of the contextual integrity approach. These principles are restrictions that regulate the flow of information guided by the informational norms. The variation in transmission principles is probably endless, but some examples will be given to illustrate what principles there are like confidentiality, where the receiving entity cannot share the information with others. Reciprocity is another principle, where the flow of information goes both ways. This is more occurring in friendships than in professional relations between a patient and a doctor. The last example to illustrate the principles of transmission is dessert, which means that entities deserve to learn about another data subject like an individual deserving to know if their lover is HIV positive. The informational norms decide which principles of transmission is relevant for the specific context. If the relevant principles prescribed by the norms are not followed, contextual integrity is being violated (Barth, Datta, Mitchell & Nissenbaum, 2006: 3).

Privacy by Design

Data protection by design is becoming more popular with regulatory frameworks and data protection practices. Data protection by design is a solution that makes the protection of data possible without having to continuously mobilize all types of data protection instruments (Bellanova, 2017: 336).

An important element of data protection by design is the use of Privacy Enhancing Technologies (PETs). PETs are technologies that are specifically aimed to protect the privacy of data subjects. PETs can be divided in two groups, as substitutes or as complements. Substitutes are technologies that aim to ensure anonymity for users and complements are technological fixes that show that the technology is complying with the data protection legislation (Bellanova, 2017: 337).

Privacy Impact Assessments (PIAs) are another key element for data protection by design. PIAs can be described as the systematic process of evaluating projects for their potential effects on people's privacy. PIAs create and distribute methods for impact assessments for environmental impact assessments as well as technological impact assessments. New measures will be tested through PIAs by public institutions, advocates and experts (Bellanova, 2017: 338).

Data protection by design forces data controllers to think about the protection of data when they develop new technologies that collect and process data and come up with technical and organizational measures that will keep the data protected (Bellanova, 2017: 339). According to Rubinstein (2011: 1421), privacy by design is a concept without a definite shape. There is no widely shared understanding or definition, but for this research, the privacy by design principles described by Cavoukian will be used to create a privacy by design with a definite shape. Privacy has always been a social norm, and it still has seen some evolvement over the years. In his research, Cavoukian (2009: 1-2) stated that privacy is not only a legal and fundamental right, it is also seen as a market imperative and in the information society we live in today, privacy is a critical trust and freedom enabler. A "design-thinking" perspective to approach creativity, innovation and competitiveness is growing, and privacy should also be approached using this perspective, according to Cavoukian (2009: 1-2). This "design-thinking" perspective is a worldview which looks to overcome issues through an innovative, holistic and interdisciplinary approach. Cavoukian tried to establish a universal framework to create the best possible protection of privacy by listing seven foundational principles of PbD.

The first principle is **Proactive not Reactive, Preventative not Remedial**. This principle states that the PbD approach anticipates and prevents privacy breaches before they can occur instead of offering privacy breach solutions. PbD commits to create and protect high privacy standards, often higher than is required of international regulation. Using this framework, methods to seek out bad privacy designs and to prevent and correct other privacy risks before they can be a problem should be established (Cavoukian, 2009: 2).

The second principle is **Privacy as Default**. PbD tries to give the best degree of privacy protection by guaranteeing that private data is automatically protected in all the IT systems. Privacy is built into the system, so an individual must do nothing to keep their data private. The purpose to use data should be specified to the individual before it is collected, the collection of private information should be limited to necessary cases and should only be used for the specified purposes and the collection of data should be kept to a minimum. Private information that is collected will be hold on to if necessary and when it is not needed anymore, it will be safely destroyed (Cavoukian, 2009: 2).

The third principle is **Privacy Embedded into Design**. Privacy needs to become a crucial element of the technologies, information architectures and operations. An approach to embedding privacy into the systems should be used, one that is open to external scrutiny. Risk and privacy impact evaluations to document privacy risks and the taken measures should be carried out and made public. Privacy must be embedded into the system without lowering the functionality (Cavoukian, 2009: 3).

The fourth principle of PbD is **Full Functionality – Positive-Sum, not Zero-Sum**. PbD tries to take all interests into account and complete all the objectives in a positive-sum way. The positive-sum manner avoids trade-offs and false dichotomies like privacy against security that are used in the zero-sum approach and shows that it is possible to achieve the goals without making trade-offs. Functionality should thus not be impaired because privacy is embedded into the system. Creativity and innovation are needed to overcome the zero-sum thinking with the protection of privacy (Cavoukian, 2009: 3).

The fifth principle of PbD is **End-to-End Security – Lifecycle Protection**. This principle entails that strong measures to protect the user's privacy are embedded into the system before the first piece of information is gathered and that personal information is destroyed after the information is used to ensure the safety of the data from start to finish. The data is thus securely managed from the beginning till the end (Cavoukian, 2009: 4).

The sixth principle is **Visibility and Transparency**. All the stakeholders should be informed and assured that the technologies, systems and business practices are operating conform the objectives and promises that were set and that they are subject to control by autonomous organizations. Users and providers should be able to investigate the operations and component parts of the organization or company. Individuals should be able to complain and make amends to create the best service and privacy protection. It is also necessary to monitor, evaluate and check the compliance with privacy policies (Cavoukian, 2009: 4).

The seventh and last principle of PbD is **Respect for User Privacy**. Operators and the creators of technologies need to make and keep the interest of the individual as their number one priority. Privacy defaults should be strong, and the technologies and systems should be made user-friendly. It is important to ask for the consent of the individuals when collecting data, provide accurate personal information, give individuals access to their personal information and try to keep evolving into the next level of appeal for the individuals (Cavoukian, 2009: 5).

The principles of PbD need to be adopted by smart cities before they create applications and technologies, because retrofitting the older privacy measures is likely to fail (Eckhoff & Wagner, 2017: 21). Smart city projects can be analysed using these PbD principles, to see if they take precautions to achieve strong privacy protection.

GDPR

The EU General Data Protection Regulation (GDPR) is a legal privacy framework, approved by the EU Parliament in 2016 and enforced in 2018. The GDPR replaces the Data Protection Directive 95/46/EC and is an effort to harmonize the laws on data privacy across Europe, protect the data privacy of all EU citizens and reshape the way organizations in all regions of Europe approach the protection of data privacy. The Data Protection Directive 95/46/EC also tried all the above, but was only a directive, so it did not have the legal power the GDPR possesses.[6]

The GDPR is in its key principles not so different from its predecessor, but there are some changes made to the policies. The main points of the GDPR will be listed below for a more comprehensive understanding and come from an educational portal aiming to provide more information on the GDPR and the article by Besik and Freytag (2019: 3) on building privacy awareness into clinical workflows.

[6] EU GDPR. (n.d.). 'The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.'. Accessed on https://eugdpr.org/

The implementation of GDPR means an extended jurisdiction, which applies to all companies within the EU. The GDPR is more applicable because it is unambiguous and applies to all data controllers and processors in the EU or outside of the EU. If an organization processing data of EU citizens is not based in the EU, they must assign a delegate in the EU.[6]

If the GDPR is being neglected by an organization, the organization can be fined up to €20 million or four percent of the annual global turnover, depending on which fine is bigger. The maximum fine can be dictated to organizations for serious violations of the regulation such as processing data without enough customer consent or the violation of the core concepts of PbD.[6]

Under the GDPR, the purpose for processing data should be specified. Data that is collected needs to be for legitimate and explicit purposes and cannot be processed in ways that is not compatible with the specified purposes. Data collection should be minimized and can only be relevant and limited to what is needed for the specified purposes. Furthermore, personal data collected shall not be saved for longer than necessary for the purpose of the personal data (Besik & Freytag, 2019: 3).

The conditions for consent have been enhanced and companies cannot use long terms and conditions filled with complicated language and information anymore. When asked for consent, it should be done through an easily accessible form which is comprehensible for a larger audience. The language used in consent forms should be clear and plain and to withdraw consent must be as simple as giving it.[7] The GDPR implements a consent check, where it is lawful to process data if the data subject has given consent to use their data for one or multiple specific purposes (Besik & Freytag, 2019: 3).

GDPR expands the rights of data subjects, such as the right to access. This implies that data subjects have the right to ask data controllers whether their data is being processed, where it is processed and for which goal it is processed. The data controller must give the data subject a free electronic copy of their personal data, which means a big step to transparency of data and working on a better power position of the data subjects.

Data subjects now have the right to make the data controller erase their data, stop further distribution of their data and halt the processing of their data by third parties. This can be done

[6] EU GDPR. (n.d.). 'The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.'. Accessed on https://eugdpr.org/
[7] EU GDPR. (n.d.). 'GDPR Key Changes'. Accessed on https://eugdpr.org/the-regulation/

when the data of the data subject is no longer relevant for its original purpose or when a data subject withdraws their consent. Data portability is another change introduce by GDPR and is the right of data subjects to ask for their personal data from one data controller and transmit the data to another data controller. The framework PbD, which has been explained above has become a part of the legal requirements of the GDPR. The principles of PbD must be present in privacy policies, and when violated, a fine will be given to the organization in violation as described earlier.

GDPR implements the requirement for data protection officers (DPO) when the processing of data calls for consistent and systematic monitoring of data subjects on a large scale. DPO's are also required when special data categories or criminal data is being processed by the concerned organization. The function of the DPO is to supervise an provide advice (Bellanova, 2017: 335). The DPO must be appointed by merit, presented with relevant resources so they can preserve their expert knowledge and are able to accomplish their tasks. DPO's also must directly report to the highest level of management and must not perform other tasks that could lead to a conflict of interests.[8]

Explanation of conceptual model

The concepts used for this research are privacy, privacy implications, privacy protection and smart cities. It has been established that smart city policies and projects have privacy implications. In order to create adequate privacy protection, it is important to consider the privacy implications. Only when policy makers are considering all the privacy implications, they can achieve adequate privacy protection when creating smart city projects and policies. The consideration of the privacy implications needs to lead to action of the policy makers to integrate and achieve privacy protection in their policies and projects. This conceptual model will test if the policy makers have assessed all the privacy implications of their project and have created privacy protection that includes all the different types of privacy. If it turns out that some projects that were investigated do not have considered all privacy implications nor are all types of privacy properly protected than this research can serve as a way to raise awareness about the flaws of the project or smart cities in general. This will not only affect the focus of this specific project but could also in turn serve as a guide for future smart city projects on how to do better regarding achieving privacy protection that includes all types of privacy.

[8] EU GDPR. (n.d.). 'GDPR Key Changes'. Accessed on https://eugdpr.org/the-regulation/

Methodology

The methodology chapter consists of the operationalization of key concepts, justify the chosen research design, elaborate on the chosen methods of data collection and data analysis and assess the limitations of this research. This chapter clarifies how this research is going to take shape and explains why certain methods are chosen. This provides validity to this research and give other researchers enough information to be able to replicate the study to check the reproducibility of this research.

Operationalization

For the described concepts to be used in this thesis operationalization is required because it allows for empirical observations to be made through the usage of these concepts. Privacy has already been conceptualised, but this part will make a distinction between privacy and data protection, operationalize the types of privacy, look at the conceptualization of consideration and security in smarty cities.

The concept of data protection and the concept of privacy are not interchangeable. From a European perspective, these two concepts are closely linked, but not identical. The term of data protection serves a broader range of interests than merely the protection of privacy, while privacy protection is not only focussing on informational privacy, but also on physical and spatial dimensions of privacy. Data protection and privacy protection have some overlap, but this is only on the informational protection of privacy and not the other types of privacy formulated in the theoretic chapter. European law increasingly treats data protection as a set of rights that are different to the rights of respecting privacy. (Bygrave, 2010: 168-169). Some examples illustrating the differences between privacy and data protection are from the European Court of Justice. The Court lets individual legal persons rely on the privacy rights, while they cannot individually rely on the law of data protection. Furthermore, all the information on identifiable or identified individuals is covered by data protection but is not necessarily included in the private life (Kokott & Sobotta, 2013: 225). Privacy of data and image is overlapping with data protection, but because this research requires a more extensive research on privacy implications, the seven types of privacy will be looked at when analysing the case study. The seven privacy types will be operationalized below.

Privacy of the person. With this type of privacy, the way in which the authenticity of the individual is protected is analysed. Are the individuals able to make their own decisions within the project without interference from outside?

Privacy of behaviour and action. For this type of privacy, the amount of protection against monitoring and controlling by outsiders is analysed. What does the project do to let individuals behave freely, without being monitored by others and without exposing sensitive topics as habits, political activities and religious practices?

Privacy of communication. This type of privacy has been operationalized by analysing what is done by the project to prevent the interception of communication or protect the privacy of people's communication. What does the project do to keep the communication of individuals private?

Privacy of data and image. To make this type of privacy measurable in the case study, the steps taken to keep the data of individuals private to others is analysed. How can the project let individuals have control over their own data and what steps does the project take to prevent the data of individuals becoming available to others?

Privacy of thoughts and feelings. This type of privacy has been operationalized by looking into what is done by the project to let individuals decide whether they want to share their feelings and give them freedom to think what they want. How does the project give the individuals the freedom to feel and think what they want without limiting them in any way?

Privacy of location and space. This type of privacy is made measurable by analysing what is done to prevent individual's spatial behaviour being tracked. What does the project do to let individuals be able to move around without being monitored? This type of privacy includes privacy in the homes, cars and workplaces of individuals, which means that it is also necessary to analyse what is done to project individual's privacy in their home, car or workplace.

Privacy of association. To make this type of privacy operational, the action taken by the project to give individuals the freedom to associate with whomever they want, and freedom of speech has been analysed. What does the project do to provide individuals with the freedom of speech and letting them associate freely with other individuals?

The definition and conceptualization of consideration used in this research is 'to think carefully about a particular fact when deciding or judging something'.[9] Consideration is viewed by multiple researches as a part of the multistage process leading to a choice (Horowitz & Louviere, 1995: 1). In the case of privacy protection when creating smart city policies or projects, the concept of consideration is thinking carefully about privacy when deciding or judging how to shape the smart city policy or project.

Conceptualizing security

The next concept that needs conceptualizing for this research is security. Security is a complicated concept, because it has multiple forms. The first form is being in the absence of a threat. This is the hypothetical situation of absolute security. The second form of security is characterized by the neutralization of threats. This form refers to being protected from threats. The third form is avoiding or not being exposed to danger. The latter two forms of security are based on the presence of threats, which means that security is often based on the things that endanger security (Zedner, 2003: 155). When trying to understand the concept of security, different levels of security should be investigated. There are three levels of security, the individual level, the state level and the level of international systems. These levels cannot be seen separately, because they are complexly connected to each other (Stone, 2009: 3). For this research, it is thus important to look at all three of the levels of security. Data of the individual should be secured, the state level of security contains the national laws with measures to secure data protection of the population and the international systems in this case refers to the GDPR, which also tries to secure the data of European citizens. The concept of security in smart cities is a genuine effort to prevent harm done to the city itself and its population through either direct or indirect measures or through both the physical and digital connections (Braun et al., 2018: 4).

Justification of the research design

The research design of this research is of a qualitative nature. Qualitative research measure indicators as well as record the behavior and attitudes of research objects/subjects which provides this research with more depth and detail. Conducting interviews is a part of qualitative methods and can open new topics that were initially not considered. This research relies on expert session interviews because experts have more expertise and knowledge on the topic than

[9] Consideration. (n.d.). In *Cambridge Online Dictionary. Accessed on https://dictionary.cambridge.org/dictionary/english/consideration*

the average civil servant, and thus can be more useful in assessing the level of consideration of privacy implications and the level of privacy protection. Using a qualitative method can reveal more individual experiences that can provide a more detailed picture of why the organizations and individuals in this research act in certain ways.

This research uses a deductive approach, because this research analyses the case based on the theories gathered in the theoretical framework. The research question is answered by analysing the interviews through the lens of the theories on privacy protection and smart cities. There are multiple frameworks on privacy protection and many researches on the issues of privacy protection in smart urban environments, so a deductive design is more effective in evaluating the cases used in this research. By creating a theoretical framework and conducting expert interviews in Dutch smart city initiatives, this research design can prove an addition to the academic literature because this type of case selection in combination with the created framework has not yet been adequately explored in research.

Logic of case selection

Four cases have been selected for this research. These cases are smart city projects located around the Netherlands. These projects have been selected with the criteria that they are operating with privacy sensitive information. This could be the deployment of camera's, the instalment of sensors or the handling of personal information. These cases have been acquired through different networks; not only were fellow students working on similar researches contacted but also the thesis supervisor provided this research with valuable contacts. This has led to the selection of four different smart city projects as cases, which are all involved with privacy and security.

In this research, a multiple case study has been chosen to answer the research question. A multiple case study allows the research to be able to analyse the data within each case, but also analyse data across different cases. The similarities and differences of the cases can be studied and understood, so the conclusions about the differences and similarities can enrich the literature on privacy protection in smart city initiatives. The evidence that is found in the multiple case study are stronger and more reliable than if only one case has been studied and provides the ability to better determine whether the findings of the research are valuable. By studying multiple cases, a broader discovery of research questions and evolution of theories is possible. The conclusions made from a multiple case study are based on different empirical findings, which creates a more convincing result (Gustafsson, 2017: 11). The multiple smart

city initiatives can be analysed individually and, on their differences and similarities with the multiple case study design. This could lead to more findings on the status of privacy protection in smart city initiatives than when the focus would only be on one smart city initiative.

Method of data collection

The method of data collection for this research is the collection of primary sources by conducting semi structured expert interviews with the project managers of the selected smart city projects. These project managers have been selected as interviewees because they have the best insights into the status of privacy protection of the projects. The interviewees are experts of the project and privacy protection, so they have more knowledge than civil servants working on those projects and can thus tell more extensively about the privacy issues and privacy protection policy. A semi structured interview provides more flexibility and can lead to more insights than a structured interview, because structured interviews are not open to changes. The interviews have been conducted in person and have been recorded for transcription. Before recording, the interviewees will be asked for their consent to be recorded. When interviewing the project managers, the questions asked will not be suggestive and provide no clues or examples, so the interviewee has no chance of becoming aware of shortcomings of their privacy protection and covering them up. As a secondary source of data collection, a document analysis was planned, but the documents are not yet open to the public. It is thus not possible to compare the findings from the interviews with the findings from the policy documents.

Interview questions

Below you can find the interview questions used in this research. For the sake of this research paper they have been listed in English although the questions that have been asked where asked in Dutch. This is because Dutch is the native language to all interviewees therefore interviewing them in Dutch provides this research with more elaborate answers because speaking in their native tongue allows the interviewees to speak more comfortably and freely.

1. Could you tell me more about the smart city project?
2. How does the project collect data?
3. How does the project handle the collected data?
4. How is the collected data being processed by the project?
5. What kind of data is collected by the project?
6. Where is the data being stored?
7. How is the data being protected?

8. To what extent is data being shared with other parties?
9. How is the privacy of the individual being protected?
10. To what extent are informational rules established within the project?

Method of data analysis

As mentioned earlier, this research is a multiple case study, where the complex series of events of policy making are the focus. The multiple case study method used for this research aims to illustrate the viewpoints, focus and considerations of the project managers of Inbraakvrije Wijk, BLV, City Lab Eindhoven and Digital Perimeter. The interviews have been analysed by looking at what types of privacy are considered and protected by the project and what types are not, and by determining whether it is in accordance with the GDPR, PbD principles and the contextual integrity theory. At first, this research has analysed whether the interviewees are aware of all the different types of privacy and privacy implications of their project. Secondly, the extent to which the project managers included all the privacy implications in their policies to prevent privacy issues from occurring have been analysed. The frameworks for evaluating privacy protection described in the theoretic framework have been used to determine whether the focus on privacy protection in the project is adequate and according to regulations and principles. The results from this analysis are enough to be able to provide an answer to the research question.

Assessment of limitations

This part will explain the possible limitations of this research which could impact the reliability and validity of the results. The first limitation of this research is the number of projects, with only four projects analysed. If more projects were to be analysed and more cities were be included into the research, this research would be able to provide a more thorough analysis that leads to results which could make it more likely that this research can be more easily generalized to other smart cities in Europe and around the world. Another limitation is that this research is dependent on the willingness of smart city initiatives to cooperate with this research. If an initiative is having troubles with privacy protection, it could be possible that they are not open to an investigation.

Not all smart cities projects are the same, so it is possible that the findings of this research cannot be generalized to all the other smart city projects in the Netherlands or across the world. It is thus a possibility that the results and insights gained from this research cannot be used for all the other smart city projects. For generalization possibilities, it is recommended to look at smart city projects in similar countries, preferably within Europe, because these countries all

must adhere to the same European regulation of the GDPR, so they have a higher chance of using similar privacy protection policies.

As been mentioned earlier in this research, it is very important to include citizens in the creation of smart city projects and policies, because they are the ones that have to deal with the changes and are the ones that have the power, if their privacy concerns are not acknowledged, to dispute or even cancel smart city projects. This research is solely focused on the governmental level of smart city policy making, so does not include citizens in the analysis. This is a limitation because it does not include all the relevant actors needed for the creation and success of smart cities.

This research looks only at the consideration of privacy implications, but there could be other factors influencing the effectivity and quality of privacy protection in a smart city. It is possible that the smart city projects included in the research lack the technology or funds to achieve adequate privacy protection. It is also possible that some smart cities or smart city projects are more susceptible to cyberattacks than others due to the resources they possess, their position in global politics or societal tensions. If other variables affecting the quality of privacy protection policies are not found in this research, this does not mean that there are no other variables affecting privacy protection policies.

Case description

Burgerparticipatiesysteem Leefbaarheid en Veiligheid (BLV)

BLV is a digital notification platform designed to create a safe and liveable neighbourhood. This platform gives the citizens the opportunity to share information with the police, municipality or other users of the platform. The notifications are being made with the use of mobile applications. In case of nuisance, suspicious situations or social problems, citizens can send out a digital warning and if needed, the police or the municipality can act immediately. The police and municipality can also send out warnings when for example a lot of burglary incidents are happening in a neighbourhood. Not too much details can be shared about this project to ensure anonymity and participation in this research.

Inbraakvrije Wijk

Inbraakvrije Wijk is a project of the ministry of Justice and Safety and Dutch Institute for Technology, Safety & Security (DITSS). The project aims to reduce burglary rates by setting up field labs in multiple neighbourhoods and applying smart innovative technology. The project has three goals: Drastically decrease the number of burglaries, increase the percentage of burglary cases solved and increase the sense of security for the citizens. The field labs are physical places where partners work to test innovative solutions for effectivity and their added value. An important step in this program is to design a neighbourhood in a way that burglary is almost impossible. The project works together with the inhabitants of the neighbourhood, companies, housing associations and the Dutch Police. The participation of inhabitants in the project is voluntarily. The new possibilities that are being worked out in the field labs are: more contact between the inhabitants of the neighbourhood, better security and information about what a inhabitant can do, smart sensors that can recognize deviant behaviour and noise that could indicate burglary a robbery or violence on the street.[10] The project started testing smart fixtures on streetlight poles. These fixtures can perceive sounds and recognize behaviour, which means they work as the eyes and ears of the outdoor area to create better insights in the safety situation. The first tests are performed inside in the project area and when the tests are successful, they are being implemented in the public space. The fixtures do not film or record sounds, but only measure sound pressure on two frequencies and use movement sensors to

[10] Inbraakvrije Wijk. (n.d.). Accessed on inbraakvrijewijk.nl

recognize walking patterns. When suspicious behaviour is recognized, multiple measures can be taken with light, sound or home automation technology (Interview Delver, 19-12-2019).

City Lab Eindhoven

City Lab Eindhoven is a smart city project that started as Living Lab Stratumseind a few years ago, but the project is being enlarged to the entire city center of Eindhoven. Living Lab Stratumseind started as a project to explore the possibilities of influencing the behavior of people. The project wanted to collect data to have proof that influencing the behavior of people works. The results were that the behavior of people could be influenced by for example smell and lighting. The project can count the number of people in an area, but also looking at the movement of people and analyzing sound. The data collection is done with the installment of camera's, movement and sound sensors. The cameras have a small box installed with software that converts the footage into statistics. The data being shared with the servers is thus not footage, only numbers stating that a certain amount of people is walking in a certain direction. The sound sensors are not recording conversations, the sensors only analyze the characteristics of sounds and compare them with a library where sounds of for example breaking glass or fireworks are stored. The project has started a test that analyzes stress in the voice of individuals without recording sound of footage, but by sending a signal to city surveillance, which are able to check if the notification was just by checking police cameras in the area of the incident (Interview Kanters, 27-01-2020).

Digital Perimeter

Digital Perimeter is a project designed to create a digital safety ring around the Johan Cruyff Arena in Amsterdam. The municipality of Amsterdam, the police and the Johan Cruyff Arena are the partners in this project. The Arena is a place with financial districts, hospitality industry and residents as well. This means that the people who visit this area do so for different reasons which in turn could lead to nuisance for the different groups visiting the area. The goal is to unburden the people visiting the area, and at the same time provide them with a passage through the area. The project wants to experiment with technologies on a small scale in the area of the Johan Cruyff Arena, so if it is working properly, other areas in the city can also benefit from it. The project consists of 5 smaller projects, which all collect data in their own way. The three main projects are a crowd monitoring system, the use of bodycams supported by 5G and facial comparison. The crowd monitoring system uses sensors to count people in a certain part of the area. This provides an open view of the density of people in the area. The 5G bodycams are

used by stewards when an incident takes place to provide extra footage on places the standard cameras cannot reach. A team will look at the footage of the bodycams in order to determine how many people should be send to the location and who these people should be. The facial comparison project captures an image of the face when an entry ticket is being scanned. From this image, the biometric data will be extracted, after which the image will be deleted. If an incident happens inside the stadium, another image will be taken of the perpetrator and that image will be compared with the biometric data saved to find out the identity of the perpetrator. All these projects are still experimenting and are not yet operational (Interview Groenink, 31-01-2020).

Analysis

Importance of anonymization

All four of the projects interviewed for this research have stated that they anonymize the collected data. The following quotes from the interviews illustrate the goals of the project managers to protect the privacy of the individual with the anonymization of data. “When information is made public, it will never contain privacy sensitive information” (Interview BLV, 22-11-2019). “Eventually, the software has to work in such an anonymized way that there is no possibility that something can be turned back, that footage can be watched and that sound recordings can be listened to” (Interview Kanters, 27-01-2020). “The individual citizen can never be traced from the piece of information in the smart city” (Interview Delver, 19-12-2020The projects City Lab Eindhoven, Inbraakvrije Wijk and Digital Perimeter use technologies that collect data without collecting data about the individuals. The data does not have to be anonymized, because it is already anonymous. “We do not collect data from individuals. I do not know whether somebody is a male or female, the age, color, I do not know” (Interview Kanters, 27-01-2020). “We do not save footage, so the pattern on itself is nothing than a x y t coordinate. From this coordinate it is impossible to deduce the identity of the individual, or you would happen to have footage of the same moment” (Interview Delver, 19-12-2019). The anonymization of data ensures the privacy for individuals. The personal data of the individual is not connected to the data in the database, which leads to the protection of an individual’s privacy according to Kitchin (2016: 8).

Privacy design integrated into the projects

PbD is clearly being seen as important to integrate into the interviewed projects. “The approach of all the experiments we do, they use the Privacy by Design principles, so Privacy by Design is the common thread in all those projects. We design technologies in such a way that it is privacy friendly” (Interview Groenink, 31-01-2020). “That you put privacy first and foremost, you do that by applying Privacy by Design principles” (Interview Delver, 19-12-2020). “The basic principles we use are Privacy by Design, a fairly new thing” (Interview Kanters, 27-01-2020). Integrating the PbD principles into the projects ensures data protection without having to continuously mobilize all types of data protection instruments (Bellanova, 2017: 336). The principles of PbD are adopted by the projects before applications and technologies are created,

which has more success than trying to retrofit the older privacy measures (Eckhoff & Wagner, 2017: 21).

Temporality

Project BLV and Digital Perimeter have commented on the importance of the temporality of the data storage. The project manager of BLV stated on the use of data: “Temporality, at the moment you have used them you have to destroy them”, “What we do now is a temporal database. But that database is being destroyed after we worked with it” (Interview BLV, 22-11-2019). The project manager of Digital Perimeter had this to say on the temporality of data usage in the projects: “We have set retention periods for all of these projects, some of them are within the AVG, I believe that is 7 days. But for this (facial comparison project) it will be removed even faster. Actually, the photo is deleted immediately, it is not even saved, and the encrypted hash, actually the hash itself, we will keep during the game at least, and perhaps a little while afterwards, just in case an incident still happened and you want to look back. But that really is a minimal number of days or will not even be a few days, which is necessary to ensure that if something happens, you can still find it.” (Interview Groenink, 31-01-2020). Temporality of data usage and storage is a rule of the GDPR, which states that personal data collected shall not be saved for longer than necessary for the purpose of the personal data (Besik & Freytag, 2019: 3). Temporality of data lowers the chance of privacy breaches, because if data is destroyed right after its use, there is a smaller amount of time in which the data can be extracted by other parties. The project manager of Inbraakvrije Wijk did not speak about the importance of temporality of data usage. It is thus unclear if the data is being stored forever or destroyed after it has no more use. If the data is not being destroyed after it has no more use, it could lead to privacy risks, with the data still available for outside parties to extract if they could enter the server of the project. City Lab Eindhoven does not destroy the collected data, because the data still serves a purpose as statistics about the city. Another reason why the data cannot be destroyed because it belongs to the public, for it has been collected in a public space. This crosses the topic of data ownership, which will be discussed later in the analysis.

Rules for data access and transparency

All projects except project Inbraakvrije Wijk have stated that they have a clear division of data access for professionals. The following quotes illustrate this finding: “Everyone has their own role, and everyone has their own access. That is also recorded, so it can be accounted for afterwards. This is called logging of data processing” (Interview BLV, 11/22/2019). “It is only

meant for a certain group of people who will work with it. These are often the people who ensure that the mobility flows run smoothly during an event or a busy occasion in the area." "But that can also be the police that supervise more, it is actually only the operational people who use that data" (Interview Groenink, 31-01-2020). The division of access is corresponding with the statement of Zhang et al. (2017: 125), which states that smart cities need to fulfil privacy and security requirements of access control to protect their collected data from unauthorised access. The projects take their data protection serious by implementing strong authorization rules for the access to data.

All interviewed projects have either talked about the importance of transparency or have been transparent about the technologies they use. Examples of this are: "Who has looked at it (reports), what has been done with it, is it recorded what has been done with a report, that has not been followed up, they call it logging. Logging of data. There is always a file to justify what has been done" (Interview BLV, 12/23/2019). "Professionals can explain the use of new technologies. Anyone working with such a system must be able to explain the used technologies. And the GDPR also says: It must be simple. If someone says I'm participating in something, then he should be able to understand what he is participating in" (Interview BLV, 12/23/2019). "So, you have to have a good story, where it instantly becomes clear how the experiment works" (Interview Groenink, 31-01-2020). Transparency is the sixth principle of PbD, together with visibility. This principle states that it is important that users and providers of data can investigate the operations of the organization collecting the data. Tips for improvements and complaints from individuals can be a road to creating the best service and privacy protection for a company (Cavoukian, 2009: 4). The fact that these projects are transparent means that their technologies and operations can be scrutinized by other parties to correct mistakes and improve the privacy protection by adjusting the operations or technologies if needed.

Reluctance to share data with outside parties and purpose specification

All the smart city projects except City Lab Eindhoven stated that they do not share collected data with other parties. Data is being shared with partners in the projects, but only for operational purposes. "It (data) will not be shared with other parties other than parties a processing agreement is signed with" (Interview BLV, 12/23/2019). "Well, we share data, if we already do it, really only within the project team." "We have actually signed an agreement in which we say we do not sell it to third parties, it is used exclusively for operational purposes

to make events run more smoothly" (Interview Groenink, 31-01-2020). "We have also agreed that we will not share data with others outside the project team. And if we share data within the project team, then all kinds of forms must be signed. And the anon-disclosure agreement, that you really only use that data for the purpose described therein" (Interview Groenink, 31-01-2020). Inbraakvrije Wijk does share data with outside parties, but only for research purposes: "No, that data stays in the smart city platform, there is only data sharing on a temporary basis for research purposes, and they really can't do anything with it other than research. In that sense, there is a very strong goal retention. Commercial companies cannot do anything with this" (Interview Delver, 19-12-2019). Although City Lab Eindhoven has the goal to make all collected data accessible to the public, they still have rules about unprocessed data: "We forbid companies to have other processors. They are prohibited to share. And when sharing takes place between the various participants in our projects, it always runs through us" (Interview Kanters, 27-01-2020). The reluctance of the projects to share data indicates that the interviewed projects are aware of the challenges related to the interconnectivity of smart cities. Multiple parties sharing and processing data can lead to privacy risks, because most parties have their own way of dealing with data, for example the difference in priorities for privacy protection in public and private organizations (Braun et al., 2018: 4-5). Private organizations can also earn profits by sharing their collected data. If collected data is being shared with third parties for secondary use without the data subjects' consent, it is hard to determine whether the privacy of the individual is being violated (Braun et al., 2018: 14). It is hard to hold the controllers accountable for their actions if their data is being transformed into new data for secondary use, because it is hard to keep track of the data once it is being leaked, disclosed, intercepted, repurposed or disassembled across data streams. These complications are being avoided by the projects by not sharing their collected data. City Lab Eindhoven does share data with the public but protects the privacy of the individual by anonymizing the data so personal information of individuals cannot be leaked or shared with third parties.

The projects have a clear purpose specification for when to collect and process data. "If there is no reason, if there is no goal retention, then we will not keep track. Only at that moment that there is a report, it is tracked where the location is of the report" (Interview BLV, 12/23/2019). The project manager of Inbraakvrije Wijk stated after the question if they shared data with outside parties: "No. Because it is only this smart city, with this purpose only. So, there is a very strong goal retention (Interview Delver, 19-12-2019). The clear purpose specification of the projects for data collection and processing prevents data from being processed in ways that

is not compatible with the specified purposes. Purpose specification also minimizes data collection by only allowing data collection that is relevant and limited to what is needed for the purpose specified by the project (Besik & Freytag, 2019: 3). A clear purpose specification for minimizing the data collection and prevention of the secondary use of data is a rule of the GDPR (Besik & Freytag, 2019: 3).

Data storage

The interviews with the smart city projects showed that all the projects save their data, or are planning to save their data on central, protected and private clouds. “It will always be secure databases, or the police system, or a foundation established for this, because something like that must be maintained. But something checked by the government. It will be a private cloud of that foundation or whatever entity it will become” (Interview BLV, 12/23/2019). “On a server that is in the town hall. So not from the municipality, the server, it is ours, from DITSS. It is in the town hall, in a secure environment, though. Made redundant with a backup system. That is where the data is” (Interview Kanters, 27-01-2020). “The smart city environment, it is a server on which fireware is installed, that is an architecture for a smart city with an open source. It is designed to receive and control an entire IoT environment. So, of course, the normal security rules apply there, applies to whatever you install on a server, the database, or with firewalls or with private networks, virtual networks and things like that” (Interview Delver, 19-12-2019). “It is in the public space which means that the municipality is responsible for it, and we have our own server room, at Central Station, 15 meters below ground, that really is a bunker.” “For those bodycams it will immediately go to the video management system of the Arena, also with facial comparison. Because it takes place there.” “Yes, that is a secure environment, you also need authorization to access it. Often also adjusted via VPN, so that is certainly secured” (Interview Groenink, 31-01-2020). The enormous amount of data stored by smart cities can cause challenges for privacy protection. When smart city projects would send their data to cloud service providers not related to their project, data breach points arise because external cloud service providers have their own standards for privacy and security. Sharing data to a third party like a cloud service provider raises consent and responsibility issues, because they have the task to handle a large amount of personal information, for which the data subject may not have given their consent (Braun et al., 2018: 12). The projects have all acknowledged the problems that could surround external cloud service providers for the storage of data, so they made the decision to store it locally, on a private and protected server. There will always be a chance that

personal information will be extracted from the storage locations, but the decision to create central, protected and private data storage make the projects less vulnerable to privacy risks.

PIAs

To determine the impact of their technologies on the privacy of the individual, the smart city projects in this research execute PIAs or DPIAs. “A DPIA is held regularly. It investigates whether the system works as designed and what can be improved. The DPIA, in which is also checked whether the procedures are followed, whether the controller can also be responsible for which he is responsible” (Interview BLV, 12/23/2019). “We are now in the middle of the DPIA, you would know what that means” (Interview Delver, 19-12-2019). “But before we do that, we still have a number of (...) and that includes going by the privacy committee, which then must perform a PIA, a privacy impact assessment” (Interview Groenink, 31-01-2020). According to Bellanova (2017: 338), PIAs are a key element for data protection by design. New measures of the smart city projects are being tested through the PIAs by public institutions, advocates and experts, which will determine the impact of the technologies on the privacy of the individual. If the technologies and measures of the smart city projects have privacy issues or will have a bad impact on privacy, they will be identified by the PIA before they are in effect and will thus not cause any harm to the privacy of individuals.

Education of individuals

An interesting result of the interviews that did not occur in the theoretical framework is the goal of educating individuals about the protection of privacy. The BLV project manager stated that “everybody should know what their own privacy and the privacy of others mean.” “You will therefore have to bring this out through commercials on TV, so if you see that, this project will be behind it” (Interview BLV, 22-11-2019). “We need to make them (individuals) aware of what that means, a lot of people do not know how important privacy is. They give away their privacy data very easily on the internet” (Interview BLV, 23-12-2019). The project manager from City Lab Eindhoven also made a point about educating individuals: “We say, the citizen has to know what data is being collected. We do think it is our task, to warn the citizen, that they are at risk, in particular because they do some things themselves” (Interview Kanters, 27-01-2020). These two projects have expressed their concerns with the privacy of individuals that is being endangered by themselves. Their opinion is that individuals play an important part in privacy protection in smart cities. When looking at new theories on educating individuals about the protection of their privacy, it was found that no specified research was conducted about this

topic. This gap in the literature matches the statement of Van Zoonen (2016: 479), stating that when developing smart city innovations or technologies, the citizens are often neglected as partners. Van Zoonen sees the importance of the support and input of the citizens, because they will be confronted with the smart city technologies in their daily lives. It is thus important to include the individual in the smart city projects, because if they give up their own privacy by mistake, the project can have adequate privacy protection and still create privacy threats to society. These privacy threats can be caused by the combination of multiple datasets. This will be further explained below.

Combining datasets

In the interview with Kanters from City Lab Eindhoven, the risks of the combination of datasets on privacy were discussed. “When you have multiple data sources, also from other locations of the municipality, because we have a monitor as a municipality, stating that in a certain neighborhood is a certain level of unemployment, or the age statistics, this many dogs and this often a trash bin is destroyed. If you put together all that data which is anonymous on itself, then it could well be that in due course you can take a picture so that only one or two possible addresses will come out. And we do think about that, I don't really think they think about it nationally, what will happen if you pull together totally anonymous sources to an excessive degree” (Interview Kanters, 27-01-2020). “The biggest leak for the average citizen is Facebook and Google, because that is where they let everything out.” “That is where the greatest danger is, with the Googles and the Facebooks. They know much more about you than the municipality, the government. (Interview Kanters, 27-01-2020). “I think that if you search a little within the publicly available sources of the municipality of Eindhoven and you combine them, for example with Google Maps and what you find on Facebook, then you can already create interesting profiles” (Interview Kanters, 27-01-2020). This illustrates the problem of combining datasets for privacy protection. Data can be completely anonymous, but it can still be possible to create profiles about individuals by combining anonymous data from the municipality with information on social media sites. This confirms the theory of Kitchin (2016: 8), stating that the problem with anonymization is that it is often not very hard to re-identify the data by using big data generation or computational technologies.

When asked the question if the project has thought about a different approach because of the risks of privacy breaches due the combination of datasets Kanters answered: “No, because we have as a starting point that data collected in the public space is available to everyone. That is

our principle. Information that the government collects, with community money, must also be public. That is not a choice, that is European legislation. Under the Data Reuse Act, it is mandatory to make data that they collect with government funds publicly available" (Interview Kanters, 27-01-2020). This means that there is a privacy breach which cannot be fixed by the smart city projects alone, because they are forced by law to make the data open to the public if it is collected in a public space. This brings us back at the topic of the education of individuals on the protection of privacy. If the smart city projects must share their data because it is owned by the public, they can do it completely anonymized and still create possibilities for privacy breaches. Individuals can prevent this privacy breach by knowing what impact the information they share on the internet has on their privacy. As project BLV and City Lab Eindhoven stated, they feel like it is their task to help the individual protect their own privacy by creating awareness about privacy risks. Without any clear legislation on what individuals can and cannot share, education of the individual is crucial for successfully protecting the privacy in smart city projects or initiatives.

If smart city projects do not take measures to help individuals protect their privacy, they do not consider all the privacy implications of their project. Not considering these privacy implications results in a possible disregard for all seven privacy types, depending on what kind of profile is created about the individual. If the profile contains locational information, there is a disregard for privacy of location and space, if the profile contains information on activities, there is a disregard for privacy of behavior and action and so on. Not realizing that the education of individuals on the protection of privacy is crucial and not taking measures to do so, means that there is a disregard for people their privacy because of privacy implications not being considered. If the smart city projects that have the obligation to make data open to the public like Digital Perimeter and City Lab Eindhoven are not aware of these privacy implications of their project and are not taking measures to educate the individual, the two projects could have a possible disregard for all types of privacy. City Lab Eindhoven spoke about the risks and solution to educate individuals, which means they consider the implications, but Digital Perimeter did not explicitly speak on this topic.

Another possible option for smart city projects to limit the privacy risk of combining datasets is carefully considering the terms of data sharing with the public. If the project would select or limit the type or number of formats, they would be able to influence the amount of parties that can work with the data (Walravens & Ballon, 2013: 75). This would make it harder for parties

to combine many datasets to make profiles about individuals, resulting in a better privacy protection.

Data ownership and control over data

From the interviews with the projects, unclarity about data ownership surfaced. “Yes, the data is from Rotterdam. There is also a question about that, during a field lab, who owns the data? Is the data from the ministry, is it from the municipality, actually I would say from the municipality, but for another reason you could say it is from the justice department until ...” (Interview Delver, 12/19/2019). “No, that is really kept within the circle, yes. Those images are not accessible to, well, maybe if you were filmed yourself, because then, of course, you own your data if you are filmed there” (Interview Groenink, 31-01-2020)."The problem with these discussions is that it is still so young in the Netherlands. There has been talk about data ownership for two years now ... but the discussion about AI and data ownership, the combination of data that is still so fresh "(Interview Kanters, 27-01-2020). These quotes illustrate that there is not yet clarity about the ownership of data collected in smart city projects. Greller & Drachsler’s (2012: 50) research confirms this result by stating that there is a lack of legal clarity concerning data ownership. In 2012, the owner of the data collection tool had the ownership of the collected data about a person before it is anonymized. The data collection was mostly done with questionnaires and sign-up processes, but nowadays ambient sensors and new technologies collect data about more parts of the behavior of data subjects without their approval or awareness, threatening the ethic principle of informed consent. The question of the data ownership of a person’s life data is very complicated but needs to be answered to ensure the protection of privacy. In their research, Al Nuaimi, Al Neyadi, Mohamed & Al-Jaroodi (2015: 9) stated that specific smart city projects have the ownership of most collected data, but a lot of the data collected includes private information of citizens. They also stated that access to this type of data is viewed as a violation of a person’s legal privacy rights by a large amount of the population. If the problem of data ownership is not being resolved the privacy of data and image is being violated. Privacy of data and image involves making sure that the data of individuals is not automatically available to others and that individuals have some control over their data and the use of it (Finn, Wright & Friedewald, 2013: 8). If there is no clear data ownership of the data collected in public spaces by smart city projects, individuals cannot have control over their data and the use of it because they do not know who has ownership of and access to their data which makes it difficult to guarantee the data is not automatically available to others. Data ownership is becoming more challenging and important because of the new

technologies collecting more and different types of data about individuals in public spaces. Not creating clear rules about data ownership is thus a disregard for privacy of data and image.

Biometrics

In the interview with Digital Perimeter the project of facial comparison was discussed. “With facial comparison, biometric data is encrypted and stored during the event.” “What we want to try with this experiment is the moment you scan your entry tickets; a photo will be made of you. Within that photo your biometric data is calculated and encrypted, the photo is immediately discarded. So, what I have is an encrypted code that cannot be traced back to something, linked to the access ticket. As a host organization I don't do anything at all, unless something happens in the stadium that is not allowed, think about lighting a torch, throwing a punch at your neighbor. Then another photo is made, which will also happen now, it will be filmed. If I have a photo again, I can make that calculation again, which I can then match with everyone who has entered the stadium. So, then I immediately have a name with the person who participated in the incident. (Interview Groenink, 31-01-2020). “We keep that encrypted hash, actually the hash itself, at least during the game, and maybe a little while afterwards, in the case there is an incident you want to look back on. But that is really a minimal amount of days or will not even be multiple days, which is necessary to ensure that if something happens, you can still find it” (Interview Groenink, 31-01-2020). This project could conflict with the privacy of the person, which is the right to keep characteristics and functions of the body private like genetic codes and biometrics (Finn, Wright & Friedewald, 2013: 8). The visitors of the stadium are entering a private area, which means that if the stadium asks for consent for collecting biometric data from the visitors, the organization would be in their right to execute this project. If the project does not ask for the consent of visitors before collecting the biometric data, it is a disregard for the privacy of the person. The measures of asking for consent must be in place before this project is in effect, or privacy risks will occur.

5G

In the interview with Digital Perimeter, the use of 5G for bodycams was discussed. “It can be a test of 5G testing, so we are going to use bodycams on 5G.” “But for another project, for those bodycams for example, where the data you collect is images, especially personal data, the privacy becomes more interesting. And they are not necessarily processed, because they are simply watched by the people who may be watching from the control room if an incident has happened. --- Because, the idea is actually to test 5G with it. Because with 5G you can move a

lot of data, much more than you could with 4G." "And with 5G you can make part of that bandwidth private, purely for the stewards in this case" (Interview Groenink, 31-01-2020). 5G is a technology that can be useful for smart city projects, by being able to cope with the growing information traffic. 5G can provide security to the entire network and provide reliable connectivity. There are some security and privacy challenges involving 5G like authorization, confidentiality of communications, access control, authentication and integrity (Catania, 2019: 26). Privacy features in the 5G system need to be considered from the start of the project and some features should be built into the system of the project. In addition, the 5G system should be smart enough to be able to adopt the privacy in accordance with the degree of importance of the services (Kumar, Liyanage, Ahmad, Braeken, and Ylianttila, 2018: 278). If the challenges of 5G systems are not considered with the implementation of this project, footage recorded by the bodycams could be intercepted by outside parties which would violate the privacy of individuals in the footage.

Discussion

When looking at the consideration for privacy implications of the smart city projects focused on in this research, it can be observed that the projects take multiple measures to protect the privacy of individuals. All four of the projects were very clear about the anonymization of collected data, so the data cannot be traced back to the individual. The projects have different measures and technologies for the anonymization of data, but the goal is the same for all. This means that the projects have considered that anonymization lessens the privacy implications of their operations. Besides the anonymization of data, PbD principles are being implemented in the projects, which causes the integration of privacy measures in the technologies used to collect data. Privacy protection is thus a priority and will not need the continuous use of data protection instruments to prevent privacy risks. Project BLV and Digital Perimeter have spoken about the importance of temporality with the use and storage of data. Destroying data after it has no more use is a rule implemented by the GDPR to prevent data breaches that are unnecessary. Project Inbraakvrije Wijk did not speak on the temporality of data, so if they do not destroy the data when it is not needed anymore, it could lead to data falling into other people's hands, meaning a disregard for privacy of data and image. People would have no more control over the data collected about them if they do not know who collects and handles their data. Although the data collected by Inbraakvrije Wijk is anonymous, it is still collected from people walking in the neighborhood, which should mean that it is at least partly their data. City Lab Eindhoven does not destroy data because they are obligated to share their data with the public. They also made

it their goal to make their data public, to inform the public and help the city with providing data about specific neighborhoods. The projects in this research deal differently with the temporality of data, which is mainly because of the difference in operations, type of data collection and whether the data is collected in public or private spaces. The interviewed projects except Inbraakvrije Wijk have stated that they have rules for the access to data. This prevents unauthorized people from accessing data. Limited access to data creates a stronger privacy protection because the data being less accessible means a lower risk of data leaks and breaches.

The projects aim to be transparent about their operations and technologies, so they can be scrutinized and are more accessible to the citizens that are participating. The projects are reluctant to share data with parties outside of the project, especially commercial parties. Data can only be shared when there is a clear purpose specification. The projects also have a clear purpose specification when collecting data, which minimizes data collection. The data storage of all projects will be done on a secured private server, assuring control over the data which could not be the case if the data was stored by an external cloud service provider. The projects are regularly executing PIAs, testing if their technologies work as predicted and to test if the technologies are not violating any privacy rules. This indicates that the projects are actively looking into the privacy implications of their technologies. The measures taken by the projects which have just been displayed are indicators that the projects have considered a lot of privacy implications they could cause with their operations. It is a positive finding to observe the emphasize the projects put on achieving good privacy protection and to see the projects have considered many of the possible privacy implications of their operations.

Besides a lot of privacy implications being considered by the projects, it has been observed that there could be some privacy implications that have not been considered. Project BLV and City Lab Eindhoven have stated that they see the importance of educating the individual on how to protect their privacy. This shows that these two projects realize that the individual is also a part in the protection of privacy and could create privacy breaches. These two projects have considered that their projects have privacy implications caused by individuals themselves. The other two projects have not spoken about the education of individuals, which could indicate that they did not consider the importance of the individual in the creation of a strong privacy protection. This could be a problem, especially when looking at the possibility of the combination of datasets. The anonymized datasets from the projects could lead to privacy breaches, if the datasets are being combined with other datasets and information individuals share about their own and other people's lives. With the combination of datasets, profiles can

be made about individuals that contain much more information than the individual would want others to know. This leads to privacy risks, and when the projects are not taking action to educate individuals about these dangers, but continue collecting data and creating datasets, there could be a possible disregard for all the types of privacy by the projects, depending on the type of profile being made about the individual. Inbraakvrije Wijk and Digital Perimeter did not share any information about plans on educating individuals on privacy protection, which could mean that they did not consider all the privacy implications of their project.

Another privacy implication not completely considered by the projects is data ownership of the collected data. There is a lack of legal clarity surrounding data ownership, and the interviews made clear that the projects do not yet have set up definite rules to determine which party is the owner and responsible for the data. If there is no agreement on the data owner of the project, there is a disregard for the privacy of data and image. This disregard is causes by the fact that individuals cannot be in control over their data if there is no agreement on which party owns their data. Without clear rules for data ownership, there is no transparency for individuals on who is controlling their data, so none of the parties can be hold accountable if something happens to the data. This problem must either be solved by the creation of legislation for smart city projects or a clear agreement in each smart city project with the involved parties. The facial comparison project from Digital Perimeter could also contain privacy implications that are not fully considered. Biometric data is extracted from photos of individuals, being saved during and shortly after the match. According to Finn, Wright & Friedewald (2013: 8), individuals have the right to keep their biometric data private, which would mean this project disregards privacy of the person. The stadium is owned by a private organization, which means that the biometric data is not being collected in the public space, so if the organization would clearly ask for consent to collect biometric data, visitors are able to make the choice of sharing their biometric data in exchange for access to the stadium themselves. But when the project fails to ask for consent of the visitors, this would deprive the visitors of the choice to share or keep their biometric data private, leading to a disregard for the privacy of the person. The last possible privacy implication that may not have been considered is the use of 5G for bodycams. 5G systems have multiple advantages or projects like Digital Perimeter, but the new system also involves some challenges that could influence the privacy protection. If these challenges are not being considered thoroughly, the privacy of the individuals being recorded by the bodycams could be violated. This could influence multiple privacy types, depending on the content of the footage.

This analysis showed that besides a lot of privacy implications being considered by the projects, there are some privacy implications not yet considered or not discussed in the interviews. Three of the four interviewed smart city projects are still in their testing phase, meaning not all the privacy implications could have been considered yet because the technologies could not yet be fully functional. Not considering all the privacy implications would not have the same consequences as for projects that are already in full effect. The projects are still testing and looking to perfect the technologies and operations, including the privacy protection. It is still important to keep exploring new possible privacy implications of the smart city projects to prevent a disregard for the privacy of individuals, with the continuous development of technologies.

Conclusion

This research aimed to identify to what extent privacy implications of smart city initiatives are being considered by policy makers. Based on a qualitative analysis of interviews with project managers of smart city initiatives, it can be concluded that the privacy implications of the smart city projects in this research are mostly considered, but there are still some implications in need of more attention before finalizing the projects. The theories used in the theoretical framework described multiple problems and threats for privacy protection in smart city environments and researchers shared their concerns with the privacy protection and information on privacy policies of smart cities. These concerns are not completely valid in the case of the researched smart city projects, because the projects take privacy protection very seriously and take multiple measures to prevent personal information falling into the hands of others. There are a few remarks that could be made about the projects, such as the absence of clear rules on data ownership, a need for more emphasize on the education of individuals and a thorough research on the use of new technologies. Technologies to protect the privacy of individuals and clear rules for data collection and processing to prevent privacy issues are being used by the smart city projects and data is not being shared with outside parties. PIA's are being conducted and the projects work closely with the data protection regulations. Principles of PbD, contextual integrity and rules of the GDPR are adopted. This way the projects minimalize the chance of privacy issues. Another interesting result is that the researched projects show a lot of similarities in the way they want to protect the collected data. Although the projects are very different from each other, the same matters are viewed as important to protect the privacy of the individual, the same techniques and the same measures are taken to prevent privacy issues from occurring. The results of this research show that the projects are careful in assessing the privacy implications and work hard to prevent any privacy issues from occurring, but there are still some issues that need to be taken care of before the projects are going to be completely operational to prevent a disregard for privacy, with privacy of data and image being the most crucial type of privacy to protect for these projects.

Limitations

The limitation of this research is that the number of analysed projects is too small to conclude on the degree of consideration for the privacy implications. It is hard to generalize the results of only a few projects to projects in other places of the Netherlands, Europe or elsewhere in the

world. This means that no real generalizable conclusions can yet be made on the state of privacy protection in smart city initiatives.

Another limitation that needs to be acknowledged is related to the method of data collection. The first two projects (BLV and Inbraakvrije Wijk) have been interviewed with interview questions that prompted socially desirable answers, which could bias the outcome of the analysis of these two projects. The interview questions have been altered after learning about the bias and the altered questions have been used in the interviews of the last two projects.

The last limitation is the unavailability of policy documents to use as secondary data. None of the projects had policy documents available to share because of confidentiality or because the documents were not finished yet. This leads to the analysis being solely based on the interviews without being able to compare the results with the policy documents. If the policy documents were available, more detailed information could be collected from the projects about their privacy protection.

This research shows that the smart city projects that have been researched are careful to achieve a proper privacy protection. Privacy issues are a big concern for individuals that are scared that in the future, they will have to give up their privacy because of the technological developments. The results of this research show that smart city projects are aware of most the privacy implications and work hard to achieve strong privacy protection policies. The results of this research could alleviate the privacy concerns of the citizens, not the fact that not all privacy implications have been considered, but the fact that the projects put a lot of emphasize on creating a strong privacy protection for the individuals participating in the projects. This result could make people more open to smart city developments, but to be able to completely earn the trust of the public, more possible privacy implications of smart city projects need to be considered. As discussed earlier in this research, smart cities or smart technologies are important to tackle the problems of overpopulation and urbanization. If more research could be provided on the state of privacy protection in smart city initiatives, the privacy concerns can be further alleviated, and lessons can be learned from the flaws of the initiatives. This brings us at the recommendations of this research.

Recommendations

More research is needed, because this research only investigated 4 smart city initiatives. As stated with the limitations of this research, if a generalizable conclusion is to be established for privacy protection in smart city initiatives, analysing a few is not enough. When more initiatives

are being researched, and the conclusions can be generalized, it can make the public more open to smart city solutions, which would lead to more efficient and better regulated cities. The analysis of privacy protection in smart city initiatives should be an ongoing process, especially with the never-ending technological developments that could open new privacy threats.

Another recommendation of this research is further research on the impact of educating individuals on privacy protection in a smart city environment. When looked at other researches relating this topic, it has been found that the literature is not adequately covering this matter. If the impact of privacy education is researched, more judgments can be made on the effectiveness for privacy protection in smart cities.

Reflection on research design

The method of semi-structured interviews for data collection have been effective for answering the research question, because it was possible to go deeper into the considerations of the policy makers and better analyse their approaches. As mentioned in the limitations, the first set of interview questions were prompting socially desirable answers, which could possibly bias the analysis of the first two projects. The used theories were clear in stating the possible privacy issues of smart city environments and provided clear frameworks to analyse the privacy protection policies of the projects.

Bibliography

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, *6*(1), 25.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE Symposium on Security and Privacy (S&P'06)* (pp. 15-pp). IEEE.

Beelen, W. (2017, June 13). 'Smart City' Den Haag zet stappen, Accessed on https://www.computable.nl/artikel/expertverslag/overheid/6374013/4573232/smart-city-den-haag-zet-stappen.html

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3), 329-347.

Besik, S. I., & Freytag, J. C. (2019). A formal approach to build privacy-awareness into clinical workflows. *SICS Software-Intensive Cyber-Physical Systems*, 1-12.

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society*, *39*, 499-507.

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200.

Catania, E. G. (2019). Security and privacy in 5G. PHD Research, Universita Degli Studi Di Catania

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*, *5*.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., ... & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Consideration. (n.d.). Cambridge Online Dictionary. Accessed on https://dictionary.cambridge.org/dictionary/english/consideration

DeCuir-Gunby, J. T., Marshall, P. L., & McCulloch, A. W. (2011). Developing and using a codebook for the analysis of interview data: An example from a professional development research project. *Field methods*, *23*(2), 136-155.

Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city—Applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 489-516.

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

EU GDPR. (n.d.). 'GDPR Key Changes'. Accessed on https://eugdpr.org/the-regulation/

EU GDPR. (n.d.). 'The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.'. Accessed on https://eugdpr.org/

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

Greller, W., & Drachsler, H. (2012). Translating learning into numbers: A generic framework for learning analytics. *Journal of Educational Technology & Society*, *15*(3), 42-57.

Höjer, M., & Wangel, J. (2015). Smart sustainable cities: definition and challenges. In *ICT innovations for sustainability* (pp. 333-349). Springer, Cham.

Horowitz, J. L., & Louviere, J. J. (1995). What is the role of consideration sets in choice modeling? *International Journal of Research in Marketing*, *12*(1), 39-54.

Jones, S. & Anderson, M. (2015, July 29). 'Global population set to hit 9.7 billion people by 2050 despite fall in fertility'. Accessed on https://www.theguardian.com/global-development/2015/jul/29/un-world-population-prospects-the-2015-revision-9-7-billion-2050-fertility

Khartoum, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51-59.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1-14.

Kitchin, R. (2016). The ethics of smart cities and urban science. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160115.

Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology*, *26*(2), 47-65.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, *3*(4), 222-228.

Koops, B. J., Newell, B. C., & Skorvánek, I. (2018). Location Tracking by Police: The Regulation of Tireless and Absolute Surveillance. *UC Irvine L. Rev.*, *9*, 635.

Kumar, T., Liyanage, M., Ahmad, I., Braeken, A., & Ylianttila, M. (2018). User privacy identity and trust in 5G. *A Comprehensive Guide to 5G Security*, 267-279.

Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Communications Magazine*, *55*(9), 16-24.

Meijer, A., & Thaens, M. (2018). Quantified street: Smart governance of urban safety. *Information polity*, *23*(1), 29-41.

Mirkin, B. (2014, April 3). 'World Population Trends Signal Dangers Ahead'. Accessed on https://yaleglobal.yale.edu/content/world-population-trends-signal-dangers-ahead

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). UAVs for smart cities: Opportunities and challenges. In *2014 International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 267-273). IEEE.

Rubinstein, I. S. (2011). Regulating privacy by design. *Berkeley Tech. LJ*, *26*, 1409.

Smith, S. (2018, March 11). 'Two billion homes needed over next 80 years, studies show'. Accessed on https://www.independent.co.uk/life-style/design/housing-crisis-global-population-increase-two-billion-new-homes-80-years-end-of-century-a8245906.html

Ståhlbröst, A., Padyab, A., Sällström, A., & Hollosi, D. (2015). Design of smart city systems from a privacy perspective. *IADIS International Journal on WWW/Internet*, *13*(1), 1-16.

Stone, M. (2009). Security according to Buzan: A comprehensive security analysis. *Security discussion papers series*, *1*, 1-11.

UN. (2014). 'The world's cities in 2016' Accessed on https://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf

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

VNG. (2018, August 13). ‘Smart City Den Haag zet stappen’. Accessed on https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/smart-society/nieuws/smart-city-den-haag-zet-stappen

Walravens, N., & Ballon, P. (2013). Platform business models for smart cities: from control and value to governance and public value. *IEEE Communications Magazine*, *51*(6), 72-79.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, *55*(1), 122-129.