Privacy in smart city Groningen:

How governments, businesses, and academics deal with it differently

10 - 07 - 2020
Erik Zuidema, S3215873
Supervisor: prof. dr. C.H. Yamu

Abstract

Smart cities are becoming more popular and prevalent, and so are the privacy issues surrounding this innovative concept. As technology and innovation progresses, privacy and security issues need to adapt. As the triple helix collaboration between governments, businesses and academics is the most important collaboration in innovation, it is important to know if these sectors regard to privacy differently or not, to find out whether privacy measures are as effective as they can be. The main question of this research therefore is: "*Do governments, businesses, and academics in smart city Groningen deal with privacy differently?"* To answer this question, a series of seven in depth, semi-structured interviews have been conducted with representatives from each of these three sectors, in which respondents were asked questions about privacy, revealing how important they considered privacy to be, as well as finding whether they carried out privacy policy. As a result, governments had a higher priority on privacy and considered it more important compared to businesses and academics. They also were more prone to carry out privacy policy, even beyond the regulations, while businesses stayed only within regulations. Thus, there is a difference between how governments, businesses, and academics deal with privacy in Groningen. Based on this result and other research, this paper suggests effective collaboration between these three sectors, to help deal with privacy issues in the future.

Table of contents

Abstract 2
Introduction 3
Theoretical framework 5
Methodology 7
Results 10
Conclusion 14
References 15
Appendix 1 17
Appendix 2 18

Introduction

Background

The smart city is an increasingly popular concept in planning. In the last decade, the term smart city has become a keyword in an increasing number of research (Figure 1). A smart city focusses not only on technology and innovation, like the digital city, but also on humans and participation (D'Auria et al. 2018). Smart city projects are associated with innovative concepts like big data and the Internet of Things , among other things (Hashem et al. 2016). These concepts deal with information collection and processing on a large scale. Some of this data is personal data, which is privacy sensitive data. While this data can help a city and its smart projects in various ways, it can also pose a threat (Xu et al. 2014). Inhabitants of a smart city are at risk of losing their privacy. As the popularity of smart cities grows, and thus the usage of new, innovative concepts as well, so did the concerns on privacy and security. Privacy protection is important, as privacy is vital in one's freedom (Rachels, 1975). This makes research into how to deal with privacy issues, especially in these new settings, important, to make sure that privacy can also be properly protected in the future.

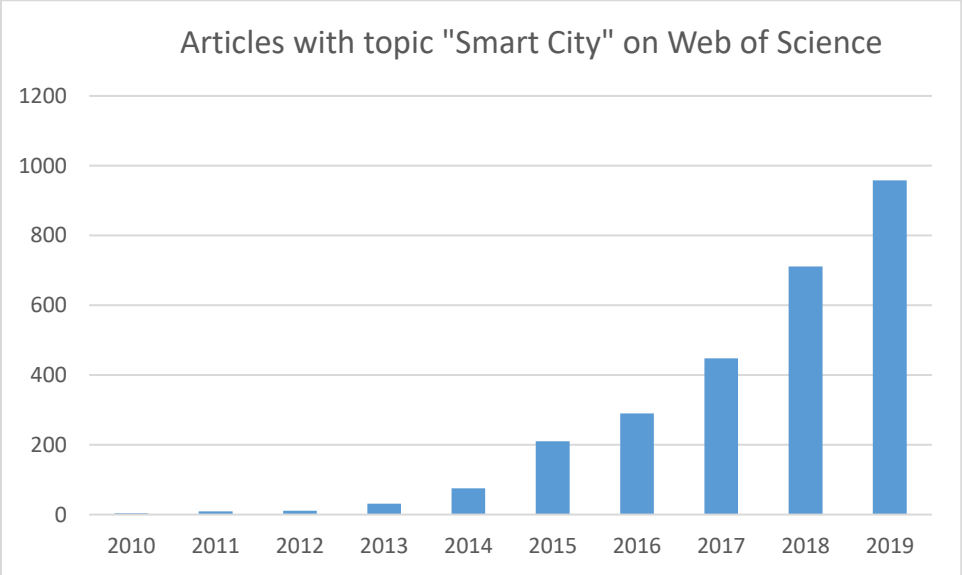

Figure 1: Usage of "Smart City" on Web of Science. Visualization by author.

Important actors

A news article by Litman-Navarro from the New York Times (2020) analyses privacy policies from large corporations. In this article, the author assessed the privacy policies of almost 150 individual companies like Facebook, Google, and Airbnb. He tested the amount of time it took to read each policy and he tested how difficult these privacy policies were to read. The results show that there is a large difference between the companies' privacy regulation on both the difficulty of reading and the time it takes to read them. The worst policy, argued by the author, was that of Airbnb, which took almost 35 minutes to read, while also requiring understanding of difficult jargon. In order to solve privacy issues in companies like these, the privacy policies need to be made clearer and more accessible for a wide public. Litman-Navarro also shows the impact of the European GDPR (General Data Protection Regulation, 2016) policy, which was implemented by Google in 2018, on their privacy policy, which became easier to understand and shorter to read, showing a need for clarity. To solve the problem that difficult privacy policies pose, strong cooperation between the relevant actors is required, thus it

is important to identify the actors, besides businesses, that are involved. According to Johnson (2008), the main actors in successful regional technological development are governments, businesses, and academics, the so-called triple helix collaboration. In smart city developments, this is the same.

Case Study

To be able to study the effects of privacy in smart cities, a case study has been carried out. This method is chosen for its ability to reveal detailed information in a case. Although this information can be difficult to generalize, it does give an indication of results in similar cases (Clifford et al., 2010). The case being studied is the city of Groningen, as it is one of two cities chosen as a lighthouse city by the making city project (Groningen - Makingcity, 2020). This project aims at making a city energy neutral, in the case of Groningen the goal is to reach this in 2035. Several of the sub-goals of the making city project make use of smart technologies. Thus, the case of Groningen was chosen due to its current situation as a smart city and its ambitions to become even smarter.

Research problem

Even though much research has been done on the relation between smart cities and security and privacy (Braun et al., 2018; Cui et al., 2018; Zhang et al., 2017), there has not been research done yet in which privacy and security perspective from governments, businesses and academics are compared. Insight into how the perspectives of actors from these sectors differ may uncover if and where inconsistencies exist, which can very well help to solve the issue privacy and security in smart cities pose (Braun et al., 2018; Cui et al., 2018; Zhang et al., 2017). The aim of this research is to find if these differences exist. Therefore, the main question of this research is as follows: "*Do governments, businesses, and academics in smart city Groningen deal with privacy differently?"* This question is split up in two parts, which are represented by two secondary questions: *"Do governments, businesses and academics think privacy is important equally?"* and *"Do governments, businesses and academics execute on privacy policy to the same extent?"* Knowing how each of these sectors feel about privacy policy and if they put the policy into practice, will give an overall view of the differences between how these three sectors deal with privacy policy. Like mentioned before, it is important to protect privacy for society. Finding out how to do this in the setting of smart cities is therefore important for the future. As said, one of the more important aspects of privacy protection is the actors involved. In the case of smart cities, these actors are academics, businesses and governments. However, research into this part of privacy regulation has not seen any research as of yet. Therefore, research into how these sectors deal with privacy issues is vital.

Structure of the current research

In the following chapters, these questions will be attempted to answer. First, the relevant theory and concepts will be explained in the theoretical framework. Then, which data collection method was chosen and why this method was chosen will be discussed, as well as the quality of the data collected. Next, the most important results of the data analysis will be given and compared to similar research. Finally, the research questions can be answered, which allows for conclusions to be drawn. Additionally, future research suggestions are given.

Theoretical framework

The smart city

One of the most important concepts in this research is the smart city, as the researched privacy concerns focus on this new setting. The article by D'Auria et al. (2018) talks about the differences and similarities between smart cities and sustainable cities. In this article, the researchers looked at the H-index, given by the web of science, of these two keywords. The article states that these two terms, against expectations, were not used together commonly. Overall, the smart city was seen as the evolution of the digital city, where the smart city differs only through the human and participation aspect it has compared to the digital city. In turn, the sustainable city was seen as the evolution of the smart city, where the sustainable city includes equity and balanced goals, unlike to the smart city. The smart city is a broad term, and can be defined in many ways, according to D'Auria et al. (2018). A general definition of a smart city is a city which uses the Internet of Things and communication technology to gather big data, which then can be used to manage resources and services efficiently. Another definition by Musa (2020) is: *'A smart city is defined as a city that engages its citizens and connects its infrastructure electronically.*' As this research focuses on the privacy and security within innovative technological projects, the technology aspect, as well as the human and participation aspect are most relevant, which both are important in the smart city, while equity and balanced goals are not necessarily as important. Thus, the smart city is the main focus of this research.

The Internet of Things and big data

The article by Hashem et al. (2016) focusses on big data and the Internet of Things and their role in smart cities. The authors state that there is still a lot left to explore when it comes to big data and the Internet of Things and their combined benefits for smart cities. Big data allows for a city to gain information from a large number of sources, while the Internet of Things connects everyday objects and devices to network technologies (Hashem et al., 2016). Each of these concepts individually may contribute to a smart city. However, the combination of these two concepts is relatively new and unexplored.

Privacy

Privacy is defined by Moone (2008) as 'a right to control access to places, locations and personal information along with use and control rights to these goods.' Privacy, as said before, is one of the major challenges of smart city implementation (Van Zoonen, 2016; Zhang et al., 2017). According to Eckhoff and Wagner (2018), this is due to a high level of complexity in people's interactions and many application areas. Due to its complexity, privacy policy may seem impossible to carry out. In their article, they state that this can lead to an unequal society. Although Khatoun and Zeadally (2017) do not talk about the dynamic between governments, businesses, and academia, they do put forward several privacy issues in different sectors, and for each of these, they propose a solution. This shows that there are many privacy issues on different scales and levels, each of which requires a specific solution.

Security

Security in the context of privacy is regarded as the protection of privacy or personal data. Although privacy focusses on all aspects of personal data, including the collection and protection, security is about protection only. Nevertheless, the problems of privacy are mostly security related, as they are

similarly complex. As a result, security gains a similar level of attention as privacy (Braun et al., 2018; Cui et al., 2018; Zhang et al., 2017).

Personal data and the AVG

Personal data is defined by the European Commission as 'any information that relates to an identified or identifiable living individual' (What is personal data?, 2020). In most cases, data must be anonymized before it can be used for analysis, as anonymization will remove the link of personal information from the data. In the Netherlands, the rules for personal data are recorded in the AVG (Algemene verordening gegevensbescherming (AVG), 2020), which is the Dutch version of the European GDPR (General Regulation Data Protection, 2016). This regulation states who may in which cases make use of personal data. In general, this use has to be transparent, the person in question needs to be informed and these data need to be protected.

Conceptual model

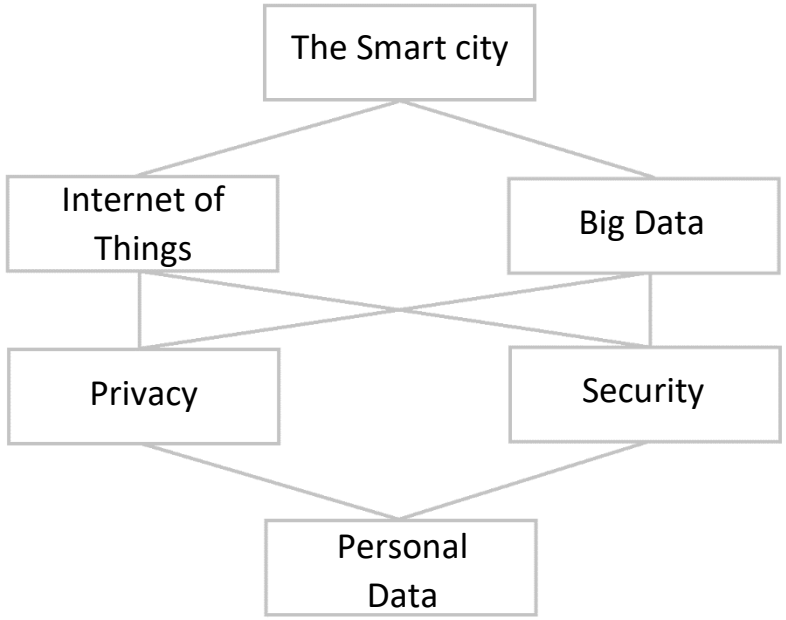

Figure 2: Conceptual model of the theory, showing all concepts in relation to each other.

The conceptual model above shows the relations between all discussed concepts and theory. The smart city at the top shows how this concept is the foundation for this research. The technologies commonly referred to in privacy issues in smart cities are the Internet of Things and big data. These two can both cause privacy and security issues. Finally, personal data follows from privacy and security, in a sense that personal data is the thing within privacy that needs to be secured.

Hypotheses

The goal of the current research is to find if governments, businesses, and academics deal with privacy in smart city projects in Groningen differently. To help find the answer to this question, some hypotheses are formulated. The first hypothesis is: Governments, businesses, and academics do not think privacy is important equally. The second hypothesis is: Governments, businesses, and academics do not execute on privacy policy to the same extent. The final hypothesis is: Governments, businesses, and academics deal with privacy differently.

Methodology

Research method

To answer the research question and secondary questions, data collection is required. This data will be gathered through a series of interviews. Each of these interviews must be conducted with respondents from one of the three perspectives of governments, businesses, and academics. These respondents also need to have experience with smart city projects in Groningen. To ensure a valid result, three interviews with respondents from each sector were intended, such that each sector is equally represented. In these interviews, respondents were asked about their take and policy on privacy when working within smart city projects.

The type of interview was a semi-structured interview (Clifford et al., 2010). This type of interview was chosen for its flexibility. The interviews followed a certain structure, but this structure could be slightly adapted during the interview, based on the responses of the respondent. This way, the researcher can gain insights that might not have followed from a more rigid interview, while still gaining insights towards the questions asked. The interview guide form can be found under Appendix 1. The interview started off with an introduction from the researcher about the interview and its subject, to make sure the respondent knows the subject. Here, the respondent was also informed about the anonymity of the interview and was asked if recording was allowed. Then, a small discussion followed where the respondent was asked about their background, followed by questions about the smart city in general. This part served to get the respondent comfortable in the interview itself, while at the same time familiarizing the subject and refreshing knowledge about smart cities. Finally, the respondent was asked questions about privacy. In this part, varying questions about privacy and security were asked. Some of these question were more directly related to the research questions than others, but the questions stimulate the respondent to think about privacy from multiple perspectives, which gives a better indication of how important a respondent considers privacy to be. This will allow for the secondary research questions to be answered individually, which can then in turn answer the main research question.

Coding

Based on the questions of the interview guide (appendix 1) and the expectations set before the interviews, a deductive code network was formulated. In this network, codes are pictured in relation to each other. These codes help ‘define what the data you are analyzing are about’ (Gibbs, 2007), thus these codes can help us answer the research questions. But before the data can be coded, interviews were transcribed, which allows for the interviews to be scanned thoroughly. After this scan, the code network was built upon (figure 3). This mix of deductive and inductive coding yields the most useful codes for analysis.

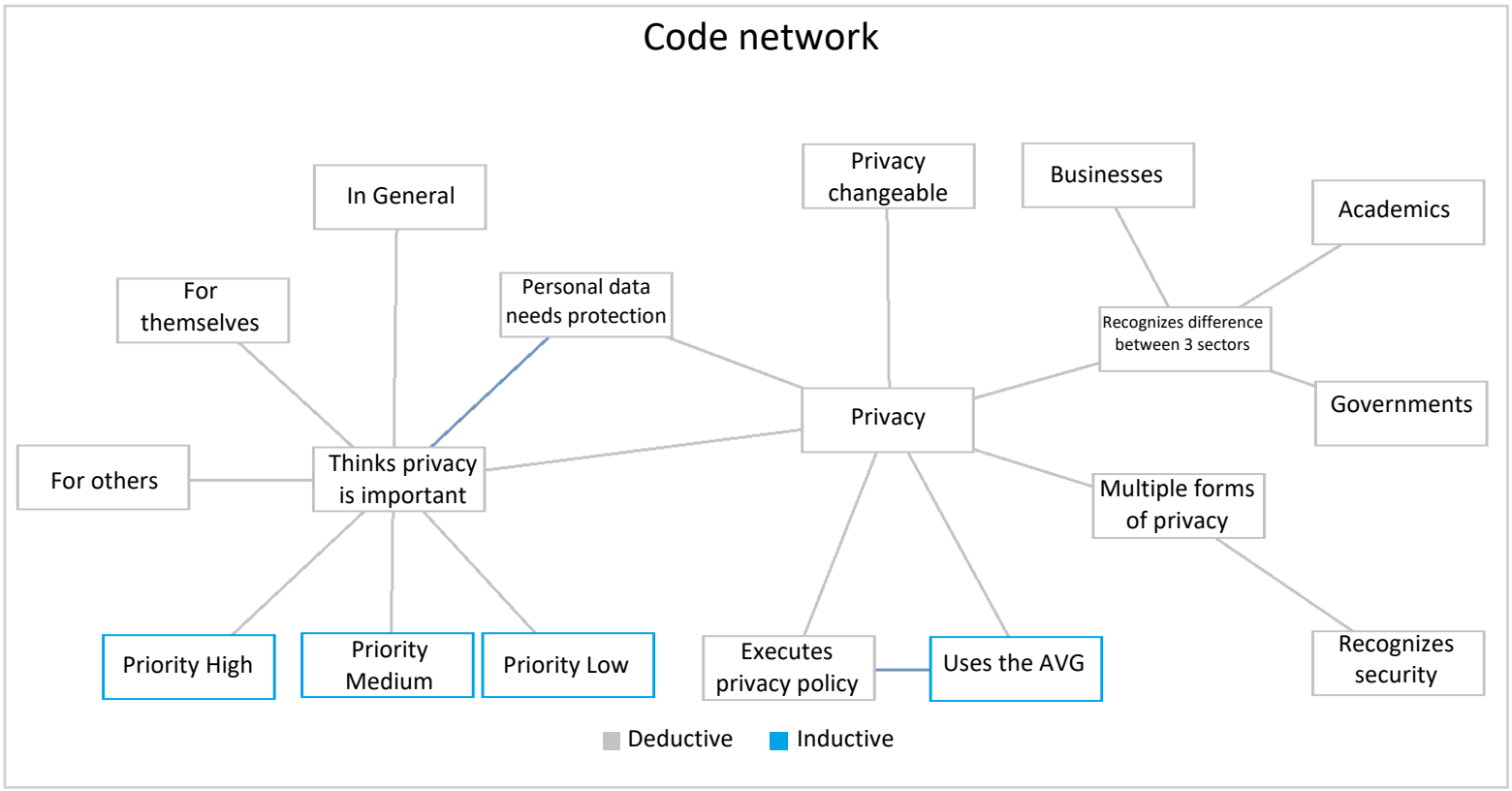

Figure 3: The code network, showing all deductive codes before the interviews and all inductive codes after the transcripts in relation to each other

Using the software atlas.ti, the transcripts were coded according to the code network. The result was a descriptive table of codes. The full table is depicted in appendix 2. In the results section, the most important findings are presented. The codes in the table can help us answer the research questions. For the question if governments, businesses, and academics execute privacy policy to the same extent, two codes were specifically designed, namely the codes 'Executes privacy policy' and 'Uses the AVG', of which the latter was inductive. For the question if governments, businesses, and academics think privacy is important equally, the codes 'Thinks privacy is important' and 'Personal data needs protection' were designed. For this second question, other codes also helped indicate how important the respondents considered privacy (High, medium, and low priority). The remainder of the codes were indicators of other questions, though they were not directly related to the research questions and will therefore not be analyzed.

Quality of the data

As mentioned before, the goal was to have three interviews with representatives of each of the three sectors. However, due to a lack of responses, only seven interviews have been conducted: three with governmental representatives, and two of both businesses and academics, even though many requests have been made. Most of which were left without response, while others refused. Some due to lack of time, others felt they were not suitable candidates. Eventually, due to time constraints, it was decided that seven interviews would have to do. Nevertheless, seven interviews were enough to preform analysis, as the respondents were still relatively well divided amongst the three sectors.

The process of inductive coding, transcribing and deductive coding proved to be an effective method. Nevertheless, the analysis proved to be more difficult. The first secondary question: *"Do governments, businesses and academics think privacy is important equally?",* had many indicative codes, which

allowed for effective analysis, as can be seen in the next chapter. However, the second question, *"Do governments, businesses and academics execute on privacy policy to the same extent?"*, only had two indicative codes, which were also recorded very few times. On the one hand this is due to the nature of the first research question being more difficult to test in an interview as compared to the other research question, since the first research question was about the thoughts and opinion of the respondents, while the second was about the practice of the respondent. On the other hand, this unfortunate result is due to a lack of targeted questions in the interview. Interview questions aimed at answering the secondary research question proved to be too vague.

Ethical considerations

As with all qualitative research, some ethical considerations were taken into account. First and foremost, as mentioned before, all data was anonymized. The interviews were recorded, with permission of the respondents, to allow for easier transcription and analysis. After each transcript had been created and analysis could begin, the recordings were destroyed. In the interviews, respondents were asked about their professional history. This however is not traceable in the analysis and the results of the research. The respondents were not selected on any basis but their expertise and field of work, nor were they treated differently in the interviews. Besides this, the Netherlands code of conduct for research integrity (Algra et al., 2018) was followed. In this code of conduct, there are five main principles, namely the principles of honesty, scrupulousness, transparency, independence and responsibility. Most importantly in ethical considerations, honesty means the researcher was truthful in explanation, using scientific sources to back up claims made in the interview questions, transparency means the goals of the interview questions were clear to the interviewee and responsibility means that the researcher has a responsibility towards the interviewee in an interview setting, with regards to privacy protection.

Important to note is that ethics are context dependent (Punch 2014). This means that in each case, in each research, the relevant ethics are different. In order to identify these relevant ethics, the researcher must stay open-minded throughout the research, while also using input from a variety of sources. Besides, Punch argues that it is important for the researcher to create an understanding of ethics, next to just achieving compliance from subjects.

Results

Equalized values for analysis

Interviews were coded, resulting in a descriptive table (appendix 2). To compare the codes to each other, their counts were totaled per sector, after which, as a result of an unequal number of interviews per sector, each sectors count was divided by the number of interviews it had, so academic and business totals were divided by 2 and government totals were divided by three. This makes it so the resulting values are comparable in a fair way.

Description interviewees

As mentioned before, the respondents were not selected on any basis except their professional background and the requirement to have been a part of a smart city project in Groningen. To protect the respondent's identity, some limited information is revealed. The respondents were all male. All of the respondents had a scientific background spread out over a wide range of subjects. Two respondents had a background in spatial planning, one in political science and sociology, one in geophysics, one in environmental sciences, one in behavioral sciences and the final respondent had a background in informatics.

Is privacy important?

For the question *"Do governments, businesses and academics think privacy is important equally?"* two codes were specifically designed, namely the codes 'Thinks privacy is important' and 'Personal data needs protection', which indicated when a respondent would express they considered privacy or personal data protection important. To the code 'Thinks privacy is important', academics noted 4, businesses noted 3.5 and governments noted 7.67. For the code 'Personal data needs protection', academics noted 3.5, businesses noted 5 and governments noted 6.67 (figure 5). This result indicates that governments mention the importance of privacy and security more often, compared to both academics and businesses. It also indicates that businesses think that personal data protection is more important than privacy, while the other two sectors think that privacy is more important than personal data protection.

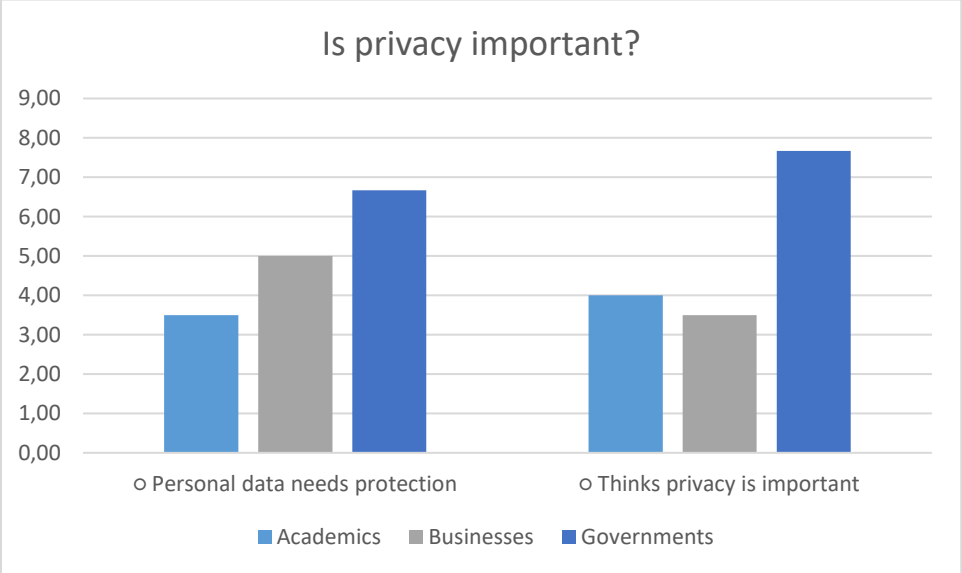

Figure 4: A visualization of the relevant codes for the question "Do governments, businesses and academics think privacy is important equally?"

How important is privacy?

Besides the previous two main codes on this secondary research question, this question had another indicator, the 'high, medium and low priority' codes, which indicated how strong the statement of the respondents was on privacy and data security. These codes were only noted when linked with one or both of the codes: 'Thinks privacy is important' and 'Personal data needs protection'. A high priority, indicating that a respondent thinks privacy or data protection is very important, was noted 0.5 for both academics and businesses and 5.33 for governments. A medium priority, indicating that a respondent considers privacy or data protection moderately important, was noted 1.5 for academics, 0.5 for businesses and 0 for governments. A low priority, indicating the respondent considered privacy or data protection unimportant, was noted 0 for academics, 3.5 for businesses and 1 for governments (figure 6). This result indicates that governments have a relatively high priority on privacy issues, meaning they stress the importance of privacy a lot. Businesses on the other hand downplay the importance of privacy issues in most cases. Academics do not downplay the importance of privacy, however, nor do they really stress the importance of privacy, and thus form a middle ground between two extremes. Academics rarely exclaimed how important they think privacy is, as they would often talk about privacy in a general sense.

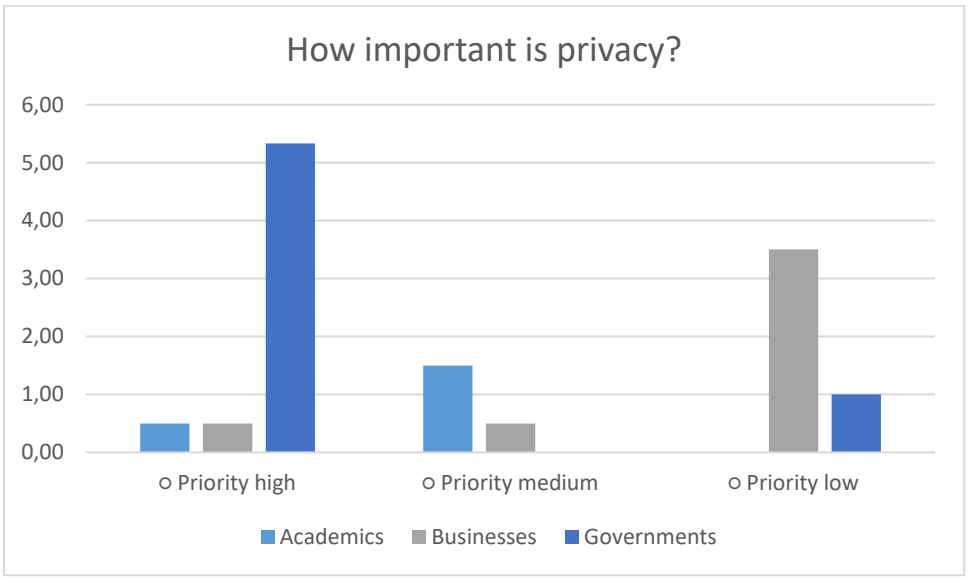

Figure 5: A visualization for the level of priority respondents appointed to privacy.

That governments considered privacy the most important was reflected by the interviews. When asked if privacy was a priority to them, a respondent from the government sector said: "[…] Maar ik merk ook gewoon bij collega's, maar ook in directieplannen, ambitieplannen, dat privacy gewoon gewaarborgd moet zijn. Ja, het zit eigenlijk, in ieder geval bij mij, gewoon in mijn denken als het ware." ([…] *But I also just notice with colleagues, but also in management plans, ambition plans, that privacy just must be guaranteed. Yes, it is, with me at least, it is just in my thinking, as it were*.) Businesses have a smaller priority on privacy. When asked the same question, a respondent from the business sector said: "Nee, privacy is sowieso niet een prioriteit. Als het al relevant is voor mij, is het gewoon nog een kwestie, zoals kosten, tijd etc." (*No, privacy is definitely not a priority. If it is relevant to me at all, it is just another matter like cost, time etc.)* Academics responded to this question by focusing on data protection from the government, which they considered most important: "[…] In termen van controle van de overheid, daar zal je goed over moeten nadenken, van hoe kan ik dat voorkomen?" ([…] *In terms of government control, you will have to think carefully about how can I prevent that?)*

Is privacy policy being carried out?

For the question *"Do governments, businesses and academics execute on privacy policy to the same extent?"* there were some issues, as mentioned in the methodology section. The most relevant codes for this question were the code 'Executes privacy policy' and 'Uses the AVG', indicating when a respondent would talk about how or when they applied privacy policies. The first code was noted 0 for both the academics and the businesses, but 1.33 for governments, while the second code noted 0.5 for academics, 2.5 for businesses and 2 for governments (figure 7). Due to the low numbers, the results are not very strong. Nevertheless, the results indicate that governments are the only sector who carry out privacy policy outside or beyond the rules set out by the AVG. Academics rarely mentioned carrying out any privacy policy, while businesses only carried out privacy policies conform the AVG regulations. The government, besides their action besides the AVG regulation, carried out even more privacy policies using the AVG.

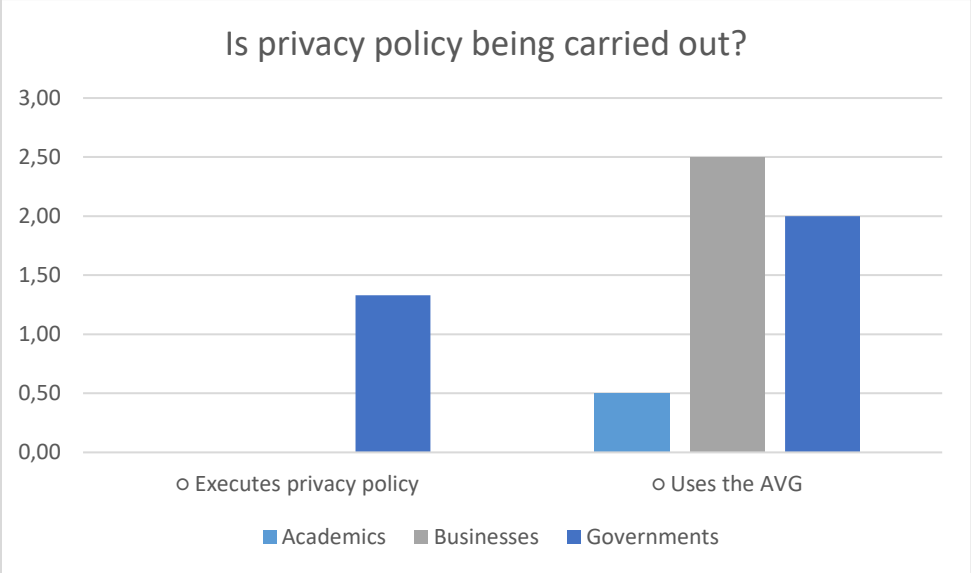

Figure 6: A visualization of the relevant codes for the question "Do governments, businesses and academics execute on privacy policy to the same extent?"

These findings were reflected by the statements that the respondents made. A government representative for example said: "Ik kan stellen dat wij, hoe wij data verzamelen, dat dat veel strenger is dan wat de landelijke regelgeving is." (*I can say that we, how we collect data, is much stricter than what national regulations are),* indicating that privacy policy is being carried out beyond the AVG, although they also use the AVG: "[…] maar dan pas je toch de gebruikelijke toetsingscriteria toe vanuit de AVG en valt het wel weer mee."([…]*but then you apply the usual assessment criteria from the GDPR and then it is not that bad.)* In contrast, businesses only apply privacy policy strictly conform the AVG. As one of the respondents from the business sector said: "Bij projecten waar we wel wat gevoelige informatie hebben houden we ons gewoon aan de regels van de AVG." *(For projects where we do have some sensitive information, we simply adhere to the rules of the GDPR.)* Academics never really went into their execution on privacy policy, as reflected by the findings.

Results of other research

As mentioned before, there are no other researches on the differences in how privacy is handled between the three sectors of academics, businesses, and governments, but there has been research done on specific parts of this question. For example, the study of Dameri et al. (2016) is about the differences between the three triple-helix sectors in smart cities. Although this study only mentions

privacy as a side note, it does lay out the differences in roles and goals of governments, businesses, and academics in smart cities. They show that, although there is a common baseline in practice, ultimately, the goals of the three sectors are simply to nonaligned. They say that to achieve long term well-being in smart cities, strong cooperation between the three sectors is necessary. This may very well also relate to privacy policy in smart cities. From the results above, it seems that the goals and ideals on privacy policy of the three sectors are not aligned in Groningen either.

In other research there is a strong focus on what should be done to deal with privacy issues. Van Zoonen (2016) for example has a strong focus on what governments should do to deal with privacy issues. Thus, in this sense, there is a lot of research from an outside perspective. However, there is no research on how important each of the government, business and academic sectors think privacy is, what they think should be done and what they actually have done / will do. Van Zoonen (2016) for example proposes action in three steps: First, identifying what privacy issues are at stake with certain technologies, like IoT. Secondly, identifying how these issues relate to EU data protection regulation. Finally, developing policy based on these privacy issues, beyond the legal limit. As they say themselves, these steps seem obvious and logical. Although it is very important to identify what needs to be done to solve privacy issues in smart cities, this analysis, as well as other research lacks in identifying willingness of actors and stakeholders. This research talks about the triple helix collaboration, the collaboration between governments, businesses and academics, thus it is believed that identifying the impact of each of these actors on privacy with respect to each other can be an important indicator for the eventual solution to privacy issues.

Conclusion

This research tried to find if there were differences between how governments, businesses and academics handled privacy policy in smart city Groningen. If such a difference exists, this could indicate that privacy policy is not equally effective in each of these sectors. To find the answer to this question, semi-structured interviews were conducted with 7 respondents from the three sectors, after which these interviews were coded and analyzed. These codes gave some strong indications on the respondent's opinions and thoughts on privacy, while they were only weak indications on the respondent's execution of privacy policy. As a result, it is likely there is a difference between how important governments, businesses and academics think privacy is, and it seems that there is also a difference in how they execute privacy policy, as it became clear from the interviews themselves that there is a difference in attitude towards privacy from the three sectors, as well as a difference in how privacy policies are being carried out. This means there is a lot to gain in privacy policy in the business and academic sectors. Thus, it is advised that future privacy policy takes this difference in attitudes between the three sectors of government, business, and academics into account. The result of the research indicates a difference in how policy is handled between the three sectors. This indicates that looking into these sectors separately when researching privacy in smart cities may yield more effective results. Because of the fact that other research suggests strong cooperation between governments, businesses and academics is necessary for effective policy, this research suggests that cooperation between the three sectors to find and fix the differences in attitude towards privacy issues between the three sectors will yield benefits in addressing these issues effectively.

Strengths and weaknesses

As all other research, this research had strengths and weaknesses. Strengths of this research were its interviews covering all three discussed sectors, which revealed some insightful data. However, this data is tainted by the unequal distribution of interviews, due to a lack of respondents. The questions asked revealed useful data for the first sub question, while revealing less useful data for the second sub question. It became clear afterwards that the interview guide missed guidance towards answers related to if privacy policy was being carried out by the respondents. The choice for a case study can be seen as a strength and a weakness. It is strong in its ability to perform a thorough analysis, although its weakness is that this may only apply to this one specific case, which is one of the reasons further research is needed.

Future research suggestions

The result of this research is only based on statements of respondents from Groningen, which may have affected the result of the research. To find whether this difference also exists in other cities, similar research needs to be conducted with respondents from those cities as well. Besides, as said before, there is no research into how the main actors governments, businesses and academics look at privacy. To support the findings of this research, there needs to be more research on how these actors together or individually deal with privacy and if their actions have effect in reducing privacy issues.

References

Algra, K., Bouter, L., Hol, A. and van Kreveld, J. (2018). *Netherlands Code Of Conduct For Research Integrity*. [online] Vsnu.nl. Available at: <https://www.vsnu.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf> (Accessed: 6 July 2020).

Autoriteitpersoonsgegevens. (2020). *Algemene Verordening Gegevensbescherming (AVG)*. [online] Available at: <https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg> (Accessed: 24 June 2020).

General Data Protection Regulation. (2016) *General Data Protection Regulation (GDPR).* [online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (Accessed: 8 July 2020).

Braun, T., Fung B.C.M., Iqbal, F. Shah, B. (2018). Security and Privacy challenges in Smart Cities. *Sustainable Cities and Society*, 39, pp.499-507.

Clifford, N., French. S. & Valentine, G. (2010). Key Methods in Geography. Second Edition.

Cui, L., Xie, G., Qu, Y., Gao, L. and Yang, Y., (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, 6, pp.46134-46145.

Dameri, R.P., Negre, E., Resenthal-Sabroux, C. (2016). Triple Helix in Smart cities: a literature review about the vision of public bodies, universities, and private companies. *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, 2016, pp. 2974-2982

D'Auria A., Tregua M., & Valejjo-Martos M. C. (2018). Modern Conceptions of Cities as Smart and Sustainable and Their Commonalities, *Sustainability*, 10(8), 2642.

Eckhoff, D. and Wagner, I., (2018). Privacy in the Smart City Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials*, 20(1), pp.489-516.

European Commission (2020). *What Is Personal Data?* [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> (Accessed: 19 June 2020).

Gibbs, G.R (2007). Analyzing qualitative data, Qualitative research kit, *SAGE Publications*, *Ltd*, London, England, (Accessed 26 June 2020), doi: 10.4135/9781849208574.

Hashem I. A. T., et al. (2016). The role of big data in smart city, *International journal of Information Management,* 36(5), pp. 748-758

Johnson, W. (2008). Roles, resources and benefits of intermediate organizations supporting triple helix collaborative R&D: The case of Precarn. *Technovation*, 28(8), pp.495-505.

Khatoun, R. and Zeadally, S., (2017). Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine*, 55(3), pp.51-59.

Litman-Navarro, K., (2020). *Opinion | We Read 150 Privacy Policies. They Were An Incomprehensible Disaster.*. [online] Nytimes.com. Available at: <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (Accessed: 7 July 2020).

Makingcity.eu. (2020). *Groningen – Making City*. [online] Available at: <http://makingcity.eu/groningen/> (Accessed: 18 June 2020).

Moone, A. (2008). Defining Privacy. *Journal of Social Philosophy*, 39(3), pp. 411-428.

Musa, D., (2020). *Smart City Roadmap*. [online] Academia.edu. Available at: <https://www.academia.edu/21181336/Smart_City_Roadmap> (Accessed: 19 June 2020).

Punch, K.F., (2014). Introduction to Social Research : Quantitative and Qualitative Approaches. 3rd ed., Los Angeles Etc., *Sage*, pp. 35–54.

Rachels, J. (1975). Why Privacy is Important. *Philosophy & Public Affairs, 4*(4), 323-333.

Xu, L. et al. (2014). Information Security in Big Data: Privacy and Data Mining. *Institute of Electrical and Electronics Engineers,* 2, pp. 1149-1176.

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

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. and Shen, X., (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, 55(1), pp.122-129.

Appendix 1

Interview guide

Inleiding

Dank u voor het nemen van de tijd en moeite om met mij te gaan zitten en spreken vandaag. Met dit interview wil ik graag meer inzicht krijgen in hoe met privacy wordt omgegaan binnen smart city projecten in Groningen. Privacy is een belangrijk onderdeel om te overwegen bij het werken met zaken als big data en het internet of things. Echter, inzicht in wat er precies wordt gedaan over privacy in dit soort projecten in Groningen is soms matig of ontbreekt in zijn geheel. Dat is iets waar ik hoop dat dit interview aan kan bijdragen.

Ter herinnering, dit interview zal worden opgenomen, zodat het achteraf beter kan worden onderzocht. Heb ik uw toestemming om het interview op te nemen?

Vragen

Dit is een interview met…, werkend/verbonden aan…

Persoonlijke vragen voor introductie

- Wat is je achtergrond, hoe ben je in ... terecht gekomen?
- Waarom werk je voor ...?

Vragen met betrekking tot smart cities, big data en het internet of things

- Wat is uw connectie met smart cities?
    - Ben je ooit Big Data of het internet of things tegengekomen?
- Werkt u momenteel aan een project met betrekking tot smart cities?
    - Zou u dat willen? Waarom?
- Wat zijn volgens u de voordelen van smart city technologieën specifiek voor Groningen?
- Wat zijn volgens u de nadelen van smart city technologieën specifiek voor Groningen?

Vragen met betrekking tot privacy binnen deze projecten

- Heeft u/Heeft u privacy in uw projecten overwogen?
    - Zo ja, hoe heeft u privacy overwogen?
    - Beschouwt u het als een prioriteit?
    - Maakt u onderscheid tussen bepaalde vormen van privacy?
- Is het privacybeleid in de loop der jaren voor u gewijzigd?
- (Hoe) ziet u privacyregelgeving in de toekomst veranderen?
- Denkt u dat bedrijven, overheden en de academische wereld anders omgaan met privacy?

Heeft u andere opmerkingen of uitspraken die niet eerder zijn genoemd of niet zijn opgedoken tijdens de vragen?

Heeft u nog tips of verbeterpunten?

Bedankt voor uw tijd.

Appendix 2

	1 - Academic	2 - Business	3 - Government	4 - Government	5 - Government	6 - Academic	7 - Business	Totals
Academia	0	0	0	3	1	1	1	6
Business	1	0	0	1	1	1	1	5
Executes privacy policy	0	0	2	1	1	0	0	4
For others	1	3	0	0	0	1	0	5
For themselves	0	2	6	1	1	1	0	11
Government	5	0	1	4	1	1	1	13
In general	2	0	1	1	0	0	0	4
Multiple forms of privacy	3	0	0	0	0	2	0	5
Personal data needs protection	3	5	12	6	2	4	5	37
Priority high	0	0	9	3	4	1	1	18
Priority low	0	5	0	2	1	0	2	10
Priority medium	0	0	0	0	0	3	1	4
Privacy changeable	1	0	1	1	1	1	1	6
Recognizes difference between 3 sectors	1	0	0	2	1	1	1	6
Recognizes security	7	0	0	1	0	2	0	10
Thinks privacy is important	3	3	13	8	2	5	4	38
Uses the AVG	0	2	0	5	1	1	3	12
Totals	27	20	45	39	17	25	21	194