The smart city trade-off

Disclosing data in exchange for smart city services

Master Thesis in
Business Information Management

Rotterdam School of Management
Erasmus University Rotterdam

Fenna Merel Levenbach
463789

Supervisors Erasmus University:
Coach: dr. Jan van Dalen
Co-reader: dr. Saskia Bayerl

Supervisor Organization: Municipality of Rotterdam
Coach: Roland van der Heijden

Date: 17-07-2017

Preface

The copyright of the master thesis rests with the author. The author is responsible for its contents. RSM is only responsible for the educational coaching and cannot be held liable for the content.

Acknowledgements

Hereby I would like to sincerely thank my thesis coach dr. Jan van Dalen and my co-reader dr. Saskia Bayerl. Jan van Dalen was always there to help when I was stuck, with critical thoughts and remarks, and guided me through the difficult times caused by the software not being on my side sometimes.
Saskia Bayerl, first of all helped fitting the research objective to my interests. Thanks to her I have been really motivated for and interested in the topic of the research through the whole project.

Also I would like to thank Roland van der Heijden, my coach at the Municipality of Rotterdam. Roland combined his knowledge and experience on, and enthusiasm for, smart city projects, to guide me through all the aspects of the Ruggedised project and the other interesting smart city projects of the Municipality.

Last, I would like to thank my family and friends. Especially Jan Brabander for reading all the way through my 'masterpiece' and for all the support, comments and energetic discussions on the topic.

Managerial Summary

The research objective of this study is to get an understanding of what residents find important in the tradeoff between disclosing data and smart city services. This is researched in order to provide urban authorities with recommendations and tools on governing privacy in smart city projects. This research steps in on challenges posed by Kool et al. (2017) on governing the digital society. Government should take its responsibility in protecting peoples' human right for privacy.

Ruggedised, a smart city project of the Municipality of Rotterdam is used as a context for the research. Ruggedised is a cooperation between the Municipality of Rotterdam, a Dutch energy provider, research institutions, businesses and other organizations. Ruggedised is a smart-grid project, with the goal to increase efficiency on energy consumption. To reach this goal energy consumption data of buildings in the smart city area is needed, which can be collected via smart meters. Next to the smart grid, the collected data at the smart city platform could be used for other purposes. Many benefits can be retrieved from collecting, storing and sharing the energy consumption data of residents, but also privacy risks are induced.

The research objective is approached exploratory by first discussing literature on how people decide on tradeoffs regarding privacy, following the Social contract framework of Milne and Gordon (1993), extended for smart cities. Within this framework the Communication Privacy Management theory of Petronio (2008) is applied to understand how people disclose information.

With the conceptual social contract framework for smart cities we test the relative importance given by residents to four attributes specified in the framework: *compensation*, *sharing*, *specificity* and *storing*. The attributes are tested via an online survey, distributed by a letter to 1200 residents of the smart city area of Rotterdam and via Facebook to residents outside Hart van Zuid. 31 residents from Hart van Zuid responded and 112 residents from elsewhere, what brings it on a total of 143 respondents.

The relative part-worth importance of the attributes are tested using choice-based conjoint(CBC) analysis. CBC is a method which let people chose between two smart meter profiles, to weight attributes with varying levels against each other.

The main findings show that residents find it relatively most important with who the data is shared, then by who the data is stored, followed by how they are compensated. The least importance is given to how often the data is updated. Figure 1 displays the results in a graph. There are no significant differences found between residents of the Ruggedised area and other residents. However there is variance between residents, which can following the Social Contract Framework be caused by differences in contractual norms between

people.

Next, the findings show that there is a strong negative effect on disclosing data to everyone in the city. There is a medium negative effect of the data being stored by the energy provider and a medium positive effect of getting a financial compensation for disclosing data to the smart city platform.

To the academic field, this research contributes to increase understanding on what residents find important in the smart city tradeoff. The study explores the applicability of the Social contract framework to smart cities.

Recommendations and tools are provided to urban authorities on how to govern smart city projects in a way that residents are prepared to disclose their data to smart city platforms. The main managerial implication for urban authorities is to give high importance to with whom the data will be shared via the smart city platform, to increase the disclosing of data and decrease privacy concerns by residents.

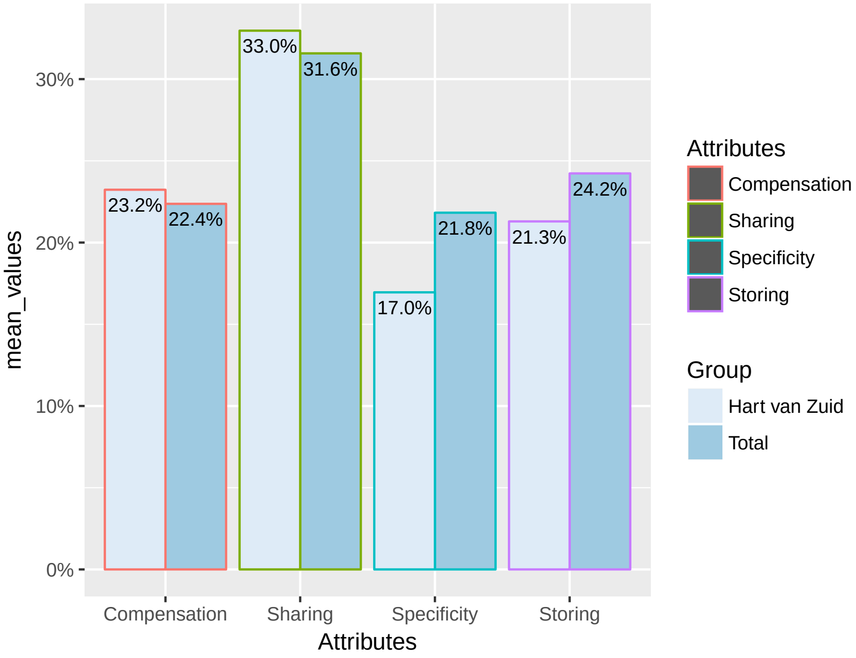


Figure 1: Relative part-worth importances per attribute

Contents

1 Introduction

Technology is everywhere around us and ready to change the environment we live in. The smart city is a concept where life quality is improved by using urban informatics and technology, to increase the efficiency of services and meet residents' needs. The city is considered smart when investments in human and social capital, and IT infrastructure contribute to sustainable growth and enhance a quality of life, through participatory governance (Caragliu et al., 2011). The smart city uses sensors and other measuring devices to collect data, and stores the data on a smart city platform. The smart city platform is a data hub where all the data is brought together.
In the smart city there are different types of stakeholders; owners, respondents and users of the data. Owners of the data could be businesses in for example city administration, education, health care, public safety, real estate, transportation, and utilities. These businesses work together and obtain and provide data to the smart city platform, where the data can be connected, analyzed and used for smart city services (Washburn et al., 2009). This research is about residents disclosing data to smart cities. The residents are cooperating in the smart city. The residents are not only users of the smart city services, but also the respondents and owners of the data.

The smart city induces several privacy risks. Personal data is easily collected and analyzed through the use of sophisticated means of the smart city. Sensors and other measurement devices on an increasing amount of objects can capture a lot of information about residents (Langheinrich, 2001). The new reality of constant surveillance causes several layers of privacy concerns. Next to the concern that surveillance creates an anxiety culture, it also leads to fears of the actual uses of the obtained personal data. For example fears of abuse and criminal misuse, errors in databases and discrimination (Zarsky, 2003). But the data can also be used by businesses and organizations to (undesirably) interfere in personal lives (McKenna et al., 2012).

The scope of this research is to understand what residents find important regarding their privacy in the smart city. Residents in a smart city exchange data for goods or services, this is called tradeoff. Users disclose information, which can be private or sensitive, and can make use of services in return. Consumers balance the tradeoff between the risks of disclosing data and the benefits by getting smart city services. They make a risk/benefit estimation to decide if and how they want to cooperate. In a smart-city this might be complicated, since it is hard to opt-out from your own city (*Slimme steden*, 2016). The Social contract framework of Milne and Gordon (1993) will serve as a basis to set out the concept of the tradeoff. Since the context of the framework regards consumer privacy in the direct mail environment, based on literature a new conceptual framework will be drafted regarding smart cities.

The Communication Privacy Management (CPM) theory of (Petronio, 2008), creates an understanding of how people decide on disclosing, private or sensitive, information. The CPM theory states that individuals develop rules to help them maximize the benefits while minimizing the risks of disclosure. The rules that are developed can stabilize over time through repeated use but are also highly situational and may be changed to fit new or evolving circumstances. Furthermore, many different rules are by people to decide what, when and to whom to disclose.
Nevertheless, the Construal Level Theory (CLT) of Trope and Liberman (2010) states that balancing the tradeoff is difficult, since privacy risks are mostly long-term risks and hard to oversee. Therefore it is useful to understand how residents of the smart city prefer to balance the tradeoff. This could help governmental organizations with developing policies regarding the tradeoff in smart city projects in order to protect residents' privacy.

Decisions on privacy tradeoffs depend on the contextual integrity. What people find important in the tradeoff depends on the context of the tradeoff (Nissenbaum, 2009). Therefore Ruggedised, a smart city project in Rotterdam, will be used to set a context for the study. Ruggedised is a cooperation of the Municipality of Rotterdam, a Dutch energy provider and multiple businesses in the smart city area called 'Hart van Zuid'. Ruggedised is a smart grid project with the goal to create a more efficient energy distribution by channeling energy between buildings in the area. The Ruggedised project will further be explained in chapter 2.
Kool et al. (2017) conclude in their research on safeguarding public values in the digital society, that attention needs to be given to fundamental ethical and social issues due to the digitization of society. Government, business and society are not ready to react on all the questions and concerns on public values and human rights such as privacy. They state that more research and effort is needed to lead the digitization in the right direction, and the government should take responsibility and leadership. To adequately protect residents' privacy, governance within the law is essential, since the smart city concept challenges the current laws and governance with new properties (Langheinrich, 2001; McKenna et al., 2012). Laws and regulations are not sufficient for protecting residents, partly because of the fast moving technology society. Concluding, local urban authorities should step in, to mitigate privacy risks of residents in smart cities.

This study is an exploratory research to determine what residents find important when balancing the tradeoff between disclosing data and smart city services.
With the results of the study recommendations and tools will be provided to urban authorities, on governing residents' privacy in smart city projects.

2 Ruggedised: a smart city project

Ruggedised is a smart grid/city project of the cities of Glasgow, Umeä and Rotterdam. The initiators of the Ruggedised project mention in their report two main tasks for the different cities:
"First and foremost, it is their task to invest, together with citizens and businesses in ensuring that buildings and whole districts will undergo a transition towards the effective and efficient use of renewable energy technologies in thermal and electricity grids, supported by smart ICT solutions, to the benefit of the citizens and to tackle climate change issues. Secondly, it is the task of RUGGEDISED cities and their partners to ensure that new possibilities to improve the quality of life of the citizens and to increase efficiency and productivity of the urban economy that arise from the unprecedented level of connectedness will contribute to economic growth."(Ruggedised, 2016, p.5).

Since Ruggedised is a project funded by the European Union, particular focus will be on creating the enabling frameworks for large-scale innovation. This includes the development and testing of new business, financing and governance models that allow for quick replication at scale (Ruggedised, 2016).

Ruggedised involves the local government, residents, research institutes, organizations and businesses. The project responds to the opportunities that arise from the integration of smart solutions. By placing sensors on a variety of objects data can be collected from different objectives in the city. The real opportunities of the smart city concept lie in combining the data from different data sources in a data platform. Gathering and combining data causes privacy risks, since the data platform is potentially dealing with personal or sensitive data. Therefore, it is essential to make agreements among the stakeholders about different aspects of privacy. Stakeholders can be the respondents, owners and/or users of the data. Several parties are working on a common goal in the smart city project, nevertheless every party has their own interests. For Ruggedised to be successful and sustainable, the importance of the preservation of privacy needs to be emphasized.

2.1 Privacy Guidelines

Several issues regarding the privacy of residents can be foreseen if residents would cooperate in the smart city. In the Ruggedised project plan it is stated that: "Privacy and security concerns will be investigated to ensure not only compliance with the local laws and standards, but also to improve the user acceptance of the solutions. The regulations regarding follower cities are also taken into account, laying a foundation for the feasibility of the solutions." (Ruggedised, 2016, p.103).

The report states that inside the boundaries of the laws regarding privacy, to achieve user acceptance and the goals of the project, creating a sustainable tradeoff between disclosing data and smart city services is essential. Since a smart city project is a cooperation of several different kind of stakeholders, this might be challenging due to possibly different stakes of each party.

2.2 Smart energy grid

In this section we will discuss the main service in the Ruggedised project, namely the smart energy grid. The idea behind the smart grid is that buildings in Hart van Zuid will exchange energy flows, with the purpose of achieving efficiency and therefore sustainability (Mohsenian-Rad et al., 2010). The project is led by a Dutch energy company, which provides the energy and places solar panels on the roofs of the buildings. Multiple businesses in the area indicated to be willing to cooperate in the smart energy grid. For example the shopping center, a big convention center, the swimming pool and other small businesses and organizations participate. The area of Hart van Zuid also contains multiple resident apartments, which could cooperate in the project.

In order to achieve the goals of the smart grid, data is needed on energy consumption of the different buildings in the area. This includes not only businesses, but also residents apartments. The energy consumption is already measured and obtained for determining energy costs, however when shared with the smart city, the data will be used and analyzed. Mohsenian-Rad et al. (2010) argue that there are no privacy risks in the smart grid service itself, since the personal data of users is not shared with other users. However, if the data is disclosed to a smart city platform, this could induce risks. Main risks lie in with who the data will be shared and since multiple parties are working together, who will store the data. The Smart City could for example have an open data platform, where users of the platform get access to the data.

If data about energy consumption is collected by the energy provider, then it should be handled in such a way that privacy is respected. The cooperation of different stakeholders in a Smart City could challenge the privacy interests of residents. The Municipality of Rotterdam should draw policies for the smart city platform to protect privacy, taking into account the preferences of the residents in the city.

3 Objective and research question

The objective of this thesis is to get an understanding of what residents find important in the tradeoff between disclosing data and smart city services, in order to provide urban authorities with recommendations and tools on governing privacy in smart city projects.
With offering services in the smart city, a tradeoff takes place between on the one side smart city services, and on the other side residents' data. In this tradeoff, residents have to weigh privacy risks against smart city benefits. To get an understanding of how decisions on tradeoffs are made by residents, we will apply the Social contract framework of (Milne and Gordon, 1993) on smart cities. The framework presents which elements are associated with the tradeoff. According to the CPM theory (Petronio, 2008), when residents have a feeling of control over the tradeoff, this mitigates privacy risks. Therefore it is important to understand what residents find important in the tradeoff, to be able to draft guidelines on privacy for smart city projects. Nevertheless, the right balance in the tradeoff should be found to achieve the goals of the smart city and on the same time preserve residents' right to privacy.

The aim of this study is to get a better understanding of what residents find important in regard to privacy, when disclosing information for smart city services. With the findings we can provide urban authorities with recommendations and tools on how to govern privacy in smart city projects. The research question of this study is:

What do residents find important when balancing the tradeoff between disclosing data and smart city services?

The present study will expand on the challenges posed by Kool et al. (2017), who conclude that government, businesses and society are not prepared for a digital society and argue that more research and effort, including in the field of privacy, is necessary to lead the digitization in the right direction. Moreover, they state that government should take responsibility and leadership in governing privacy in smart city projects. In the coming years more cities will follow with smart city concepts, therefore it is essential to attach importance to privacy from the beginning of the digitization of society. Other municipalities and governmental organizations working on smart city projects can learn from the findings and adapt these in their governing on privacy.

First this study will review theoretical frameworks on privacy and motivations in tradeoffs using the Social contract framework (Milne and Gordon, 1993) a basis, to establish how people decide on disclosing information. Based on findings from the literature and the context of the Ruggedised project, we will perform a conjoint analysis to explore to what residents attach importance regarding the tradeoff of privacy and smart city services. The choice-based conjoint analysis will be conducted via an survey to reach as many residents from Hart van Zuid, the smart city area. The main part of the questionnaire covers choice tasks where residents can choose their preferred shape of the smart city service, based on varying attributes. In this way the importance of different attributes concerning smart city services can be established. After the choice-tasks some additional questions will be asked to get a broader view on the opinion of residents on the tradeoff.

The results will provide insights in what residents find important when balancing the smart city tradeoff, indicating the relative importance attached to separate attributes regarding smart cities services.
Based on the results, the study will give recommendations and tools to urban authorities on how to govern privacy in smart city projects.

4 Theoretical background

This chapter sets out different elements of the privacy tradeoff in smart cities, in order to understand what attributes could be important for residents.
First the Social contract framework of Milne and Gordon (1993) will be presented to explain the concept of privacy tradeoffs. We discuss to which extent this framework could be applicable on Smart Cities. Then we discuss why smart cities are different than e-mail marketing and review literature regarding tradeoffs in smart cities. Last, we draft a new conceptual Social contract framework for smart cities.

Milne and Gordon (1993) researched privacy and trade-offs. They designed the framework presented in Figure 2, regarding consumer privacy in the direct e-mail environment. The social contract is an offer via e-mail in this framework. The purpose of the framework is to get an understanding of the tradeoff made in e-mail marketing. The social contract is defined by attributes, this is the stake of the tradeoff. Furthermore, the tradeoff about the social contract is between two parties: the consumer and the soliciting organization, and influenced by contractual norms which are formed by the two parties and the government. Next, the tradeoff is indirectly influenced by other businesses and organizations connected the soliciting organization, who can directly e-mail the consumer. The explanation of the lines in the framework by (Milne and Gordon, 1993, p. 207) is: "The solid lines represent the exchange of information for offers via e-mail. The bold lines represent the trade-offs consumers and organizations consider before entering a social contract, and the dotted lines represent the communication channels among various publics (consumers, government, and soliciting organizations) in this system."

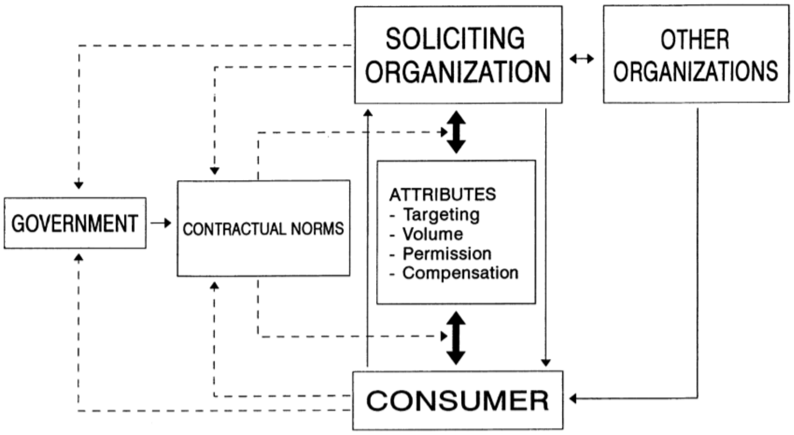


Figure 2: Social contract framework for direct marketing (Milne and Gordon, 1993)

Figure 2 shows that organizations collect information about consumers, to provide consumers with offers that may be of interest. Organizations may share the retrieved information from consumers, such as their e-mail address, with other organizations with the same goals. The tradeoff of the consumer's decision to disclose information to the organization and the organization's decision to provide the consumer with offers, are based on evaluations of both parties of the attributes of the specific social contract. The evaluation of the attributes of a social contract is governed by contractual norms. Norms are defined as shared expectations about behavior (Heide and John, 1992). Milne and Gordon (1993) state that inconsistency in the results on the tradeoff can partly be caused by evolving norms and individual differences in the salience of the norms. Nevertheless, they argue that governance is focused on the majority of individuals.

The tradeoff in the smart city is comparable. The residents have to decide about disclosing information to the smart city platform (instead of 'soliciting organization'), depending on the social contract. The data collected on the smart city platform, might be shared with other organizations connected to the platform, which indirectly influences the tradeoff. Moreover, the tradeoff is governed by contractual norms.

In this research we will use the Social contract framework to gain understanding of the tradeoff in smart cities. The research objective of this study to gain understanding of what residents find important in the tradeoff in order to provide urban authorities with recommendations on how to govern residents' privacy, therefore the focus will lie on the consumer/resident in the framework.

However, to apply the framework on smart cities, we will first have to discuss the differences between a tradeoff in e-mail marketing and in a smart city. The case of the smart city is different and more complex than the case of e-mail marketing.

First of all, in the smart city the collected data can not only be used for the same purpose, but also for other purposes by different kind of parties (Washburn et al., 2009). Therefore the risks and the benefits might differ per purpose and party. We will discuss the properties of smart cities in Section 4.1, taking the Ruggedised project as an example to illustrate the differences.

Secondly, the contractual norms differ for the context of smart cities differ. To get a better understanding of the tradeoff in smart cities it is important to review the concerned norms which influence the tradeoff. Therefore we discuss the Communication Privacy Theory of (Petronio, 2008) in Section 4.2 to understand peoples' norms on how they disclose (personal or sensitive) information. Not only the legal norms are different regarding privacy for smart cities than for e-mail marketing, also the legal norms changed since the research of (Milne and Gordon, 1993). This will be discussed in Section 4.3.

Thirdly, the kind of data disclosed to the smart city is different than in e-mail marketing. As mentioned, the data will be collected at the smart city platform, and from there on it can be used for different purposes. Depending on the purpose the type of the data might differ. For some purposes personal data is

needed, for other purposes anonymized data might be sufficient. The type of the data has influence on privacy risks as well as on smart city benefits and will therefore be discussed in Section 4.4.
Fourthly, the attributes concerning the tradeoff regarding the direct e-mails are *targeting*, *volume*, *permission* and *compensation*. Targeting, volume and permission are based on literature about disclosing information in e-mail marketing and therefore might differ for smart cities. Nevertheless, *compensation* is an interesting attribute, since this does not induce risks and might mitigate the privacy concerns people experience. We discuss this attribute in Section 4.5.

After reviewing literature about tradeoffs in smart cities, we draft a conceptual Social Contract Framework for smart cities, with attributes applicable for smart cities based on the discussed literature on the tradeoff. The attributes and the framework are presented in Section 4.6.

4.1 Properties of a smart city

Using Ruggedised as the context, the study will explore what residents find important when they disclose information in exchange for smart city services. In this section we will discuss the definition of the smart city and the properties of smart cities. Then we discuss the benefits and risks of energy consumption data, which is needed for the Ruggedised smart city project, to illustrate why the data for smart city platforms is different than for example data concerned with e-mail marketing.

4.1.1 Smart city

The smart city is a concept where life quality is improved by using urban informatics and technology, to increase the efficiency of services and meet residents' needs. The city is considered smart when investments in human and social capital, and IT infrastructure contribute to sustainable growth and enhance a quality of life, through participatory governance (Caragliu et al., 2011). In the smart city sensors and other measuring devices collect data, then the data is send via a certain connection to the smart city platform. The smart city platform is a data hub where all the collected data is brought together and stored. By bringing data from several sources together, the data can be combined. Collecting, organizing, storing and sharing of data changes the uses to which such data can be put, which induces benefits and risks (Strandburg, 2014). The data stored at the smart city platform can increase knowledge on for example the residents of the city but thereby could also provide deeply personal pictures of individual lives (Ramirez, 2013; Murphy, 2015). Hereby the data enables a lot of inference beyond the data generated to reveal insights that have never been disclosed (Kitchin, 2016). Other risks are induced by storing all the data together. For example abuse and criminal misuse of the data, errors in databases and discrimination (Zarsky, 2003). Anyone connected to the platform can obtain and use the data. Nevertheless, the platform might have restrictions on with who which data is shared. In this way several privacy layers can be incorporated.

4.1.2 Energy consumption data

The purpose of the Ruggedised project is to exchange energy between buildings, in order to save energy and create a sustainable city. To accomplish this, energy consumption data has to be collected, which can be done via 'smart meters'.
The smart meter is a new meter which will eventually replace the traditional energy meter. The smart meter is digital and registers the energy consumption by its own. In this way the results of the meter can be sent automatically to ones energy provider. Smart meters are being installed in an increasing number of homes due to the benefits they are expected to bring to the energy supply industry and its customers.
The energy suppliers expect to reduce operational overhead associated with manual meter reading and potentially improve customer loyalty (Rogai, 2006). The operators of the transmission system and distribution networks hope to benefit from a more flexible demand side to enable greater penetrations of low-carbon technologies (Strbac et al., 2010). Governments expect that the improvements in energy efficiency promised by smart meters, will help to achieve energy reduction targets. Last, consumers could benefit from reduced energy bills as they become more energy aware (Darby et al., 2006; MacDonald, 2007; Owen and Ward, 2006). Smart Meters are undergoing a period of rapid growth and collect an increasing amount of data from a growing number of households.

The smart city can use the data of smart meters for several purposes. First, for the smart energy grid the energy consumption data is needed of multiple buildings. These building might not all be contracted with the same energy provider. Therefore the data has to be collected, stored, aggregated and analyzed somewhere. Besides for the smart grid, the data of the smart meter can be used for multiple other purposes. For example, on the smart city platform energy consumption data of all the households in the city can be brought together to let people compare their consumption with similar households. Next the police can use it in cases to track down weed plantations, for which a lot of extra energy is needed or could use it in other cases to find out if someone was home for example. On top of these examples a lot more might be possible. If the data is gathered, businesses and start-ups could find different purposes for the data. A nice real-life example of data in the smart city used for unexpected purposes, occurred this year in Rotterdam. Data of the amount of garbage in containers is collected in order to optimize waste collection. Besides optimizing this process nursing homes profit from this data, since they have tight schedules and benefit from knowing when the container is empty.

So far we discussed the benefits of collecting and analyzing the smart meter data. With the vast increase in data generated by the use of smart electricity meters, important issues of privacy and data protection arise which are researched by McKenna et al. (2012). They made a summary of privacy concerns related to smart meters. This summary is presented in Table 1.

Table 1: Privacy concerns smart meters (McKenna et al., 2012)

Application group	Example concerns
Illegal uses	Burglars finding out when homes are unoccupied. Stalkers tracking the movements of their victims.
Commercial uses	Targeted advertising: Use of individual or aggregated household smart meter data to target advertising at a specific household or individual. Note: use of aggregated or ’anonymous’ data may be more acceptable than use of individual household data. Insurance adjusting e.g. do you tend to leave your appliances on when away from home?
Uses by law enforcement agencies	Detection of illegal activities e.g. sweatshops, unlicensed commercial activities, drug production. Verifying defendant’s claims e.g. that they were ’at home all evening’.
Uses by other parties for legal purposes	In a custody battle: do you leave your child home alone? In a landlord-tenant dispute: is the property over-occupied?
Use by family members and other co-inhabitants	One person in the household ’spying’ on another e.g. parents checking if their children are sleeping or staying up late playing video games. Partners investigating each others’ behavior.

Concluding, collecting the smart meter data on a smart city platform, induces benefits as well as risks which differ per purpose the data is used for. Risks for the smart city platform lie in combining, storing and sharing of the data.

4.2 Communication Privacy Management (CPM)

In this section we discuss the Communication Privacy Management (CPM) theory of Petronio (2008) to understand people's personal norms regarding tradeoffs.

The CPM theory is an extension of the Communication Boundary Management (CBM) theory (Petronio, 1991). The CPM theory has been designed by Petronio and Altman (2002) to develop an evidence-based understanding of how people make decisions about disclosing private information within personal relationships (Petronio, 2004; 2010; Thompson et al., 2012; Durham, 2008). However, the CPM theory has expanded to explain disclosure of information within other settings, including group, organizational and institutional relationships. Moreover, Petronio and Altman (2002) and others have discussed the applicability of CPM to privacy issues generated by new technologies, for example the Internet (Metzger, 2007; Stanton and Stam, 2002; West and Turner, 2013). Metzger (2007) explains this applicability by three premises. First, benefits and risks to disclosure also exist in the digital context. Benefits in smart cities may include sustainability, faster services and lower prices. Risks include theft and surveillance. Second, studies found that people feel ownership over the personal information they provide digitally as well as in personal relations and believe they have the right to control access to personal information shared online (United-States-Federal-Trade-Commission, 1998).

Petronio (2012) states that privacy is defined by the feeling that one has the right to own private information. The CPM theory suggests that individuals maintain and coordinate privacy boundaries (the limits of what they are willing to share) depending on the perceived benefits and costs of information disclosure. People must balance their competing needs for privacy and for disclosure. She introduces privacy boundaries, which allow people to control who has access to the information and motivate to set expectations for co-ownership of information.

The CPM theory is composed of five principles; ownership, control, co-ownership, privacy rules, and turbulences and breakdowns. We will further discuss these principles.

Ownership

First, people believe they own and have a right to control their private information (Petronio, 2012). Hereby ownership is linked to control of private information. When people perceive information as their own, they want to have control. People's sense of ownership motivates to create boundaries that will control the spread of private information.

Control

People control their private information through the use of personal privacy rules. These rules are dependent on culture, gender, motivation, context and risk/benefit ratios. (Petronio, 2012)

Co-ownership

Third, when others are told or given access to a person's private information, they become co-owners of that information (Petronio, 2012). The act of disclosing private information creates a confidant and draws that person into a collective privacy boundary, whether willingly or reluctantly. Co-ownership has a collective privacy boundary which cannot be solely personal again, since the information is disclosed. Co-owners will tend to feel a sense of responsibility for the information, but the boundaries of all owners might not be evenly thick. This could for example be the case when residents share their information with companies operating in the smart city.

Privacy rules

The fourth principle states: co-owners of private information need to negotiate mutually agreeable privacy rules about telling information to others (Petronio, 2012). Where the first three principles were descriptive in how people handle private information, the fourth principle assumes that the privacy boundaries of co-owners will not necessarily look the same. Therefore this principle is a plea for co-owners to negotiate mutual privacy boundaries. These negotiations focus on boundary ownership, boundary linkage and boundary permeability.

Boundary ownership consists of the rights and responsibilities co-owners of private information have to control its spread. In smart cities residents will perceive ownership of their private information, this ownership might shift when businesses obtain this information to offer services. The information is then stored in databases of the businesses and they become co-owners.

Boundary linkage is an alliance formed by co-owners of private information as to who else should be able to know the information. In the smart city this might be the case when, for offering extra service another company who does not obtain the data oneself, needs to be included.

Boundary permeability is the extent to which a boundary permits private information to flow to third parties. The businesses in the smart city who obtained data from residents, might want to sell your data to other companies.

Turbulences or regulation breakdowns
Fifth, when co-owners of private information do not effectively negotiate and follow mutually held privacy rules, boundary turbulence is a likely result Petronio (2012). With boundary turbulence is meant disruption of privacy management and relational trust that occurs when collective privacy boundaries are not synchronized. This boundary turbulence can have multiple causes. For example, the boundaries could not have been clear to all co-owners or there a mistake has been made. This can affect the relation ship of trust. In smart cities it is important to have the trust of the residents in order to achieve user acceptance (Sanchez et al., 2011).

Concluding, the CPM theory is predicated on five principles of private information management that represent organizing tenets interlinking both individuals and collectives: ownership of information, control, regulation through privacy rules, co-ownership of another's private information, and turbulences or regulation of privacy breakdowns (Petronio, 2012). These principles help understand why residents will or will not disclose their information. People want to have control over disclosing their information for smart city services. Since this could be hard in the smart city, this could decrease information disclosure by people. Next, people want the co-owners of their information to have the same privacy boundaries, therefore disclosing data to the smart city platform would increase when people trust the cooperating parties connected to the platform. Last people take into account turbulences and breakdowns. If personal data was misused or people are afraid for misuse by a party connected to the platform, this creates turbulence which will decrease disclosing data by people.

4.3 Privacy: laws, principles and concepts

In this section the legal norms around privacy will be reviewed and the principles and concepts they are based on, in order to get an understanding of how the tradeoff in smart cities is so far controlled by the government and judicial authorities.
Warren and Brandeis (1890) defined privacy as 'the right to be let alone'. Nowadays, a more common perspective on privacy is 'the right to select what personal information about me is known to what people' (Westin, 1967). Westin (1968) developed a framework for privacy consisting of seven principles: Openness and transparency, Individual participation, Collection limitation, Data quality, Use limitation, Reasonable security and Accountability. These principles are used to control the flow of information. First, *openness and transparency*; there should be no secret collecting of data. This refers to the publication of the existence of such collections, as well as their contents. Second,

individual participation; the subject of a record should be able to get insights in the collected data and adjust the data if it is wrong. Third, *collection limitation*; data collection should be proportional and not excessive compared to the purpose of collecting. Fourth, *data quality*; data should be relevant to the purposes for which they are collected and should be kept up to date. Fifth, *use limitation*; data should only be used for their specific purpose by authorized people. Sixth, *reasonable security*; adequate security should protect the data, according to the sensitivity of the data collected. And seventh, *accountability*; record keepers are accountable for compliance with the other principles.

These seven principles of Westin (1967) were later translated in the notion of "fair information" practices. Most laws are based on these practices, among The Dutch law 'Wet Bescherming Persoonsgegevens (Law of protecting personal data)', which states that the data of Dutch residents can only be obtained for specific justifiable purposes. This implies that it is only allowed to collect data for a well defined purpose , only data relevant for the purpose (no over collection) and only keep data for the duration it is necessary for the purpose. On top of that, the resident is required to be notified of the data being collected and the organization or person who obtains the data.

The General Data Protection Regulation (GDPR) is the new European privacy regulation. The regulation is introduced and approved in May, 2016 and the law will be maintained from May, 2018. The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Wet Bescherming Persoonsgegevens.
One important change regarding smart cities, is the stricter rules about giving consent. "Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and organizations will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given. Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data." (Regulation, 2016, L. 119/6).

When applying these laws to smart cities, we need take into account that we are dealing with new properties, caused by ubiquitous computing(Weiser, 1991). Ubiquitous computing is a concept in software engineering and computer science. There are several properties in which ubiquitous computing differs from normal computing. First, ubiquitous computing is made to appear anytime and everywhere. The second property is the invisibility of the computers. Computers are getting smaller and are not always noticeable anymore. Third, sensors are getting more accurate and smarter. Next generation sensors will allow high quality audio and video feeds from cameras and microphones smaller

than ever. This makes it possible to measure for example emotions and stress. The last property, memory amplification, enables sensory equipment to continuously and unobtrusively record every action, utterance or movement. The properties are applicable for smart cities and create challenges in enforcing the law.
Following the fair information practices and taking into account these added properties, Langheinrich (2001) identifies seven main areas of innovation and system design: Notice, choice and consent, anonymity and pseudonymity, proximity and locality, adequate security, and access and recourse. These areas will be explained in Table 2, together with the challenges induced by the smart city concept.

We can conclude that the current laws are challenged by the smart city, by introducing new properties in data projects. Since the smart city induces challenges to the current laws and the new privacy laws are not enforced yet, this could cause different individual interpretations of the legal norms. This might influence the results of the tradeoff (Milne and Gordon, 1993).

Table 2: Privacy by design smart city

Privacy by design (Langheinrich, 2001)	Explanation	Challenges Smart city
Notice	Users should be notified about the data being collected. Langheinrich (2001) suggests some kind of announcement system, depending on the type of device.	Devices and sensors might not support a tactile interface.
Choice and consent	Following the enactment of the EU directive, it's not enough to just announce and declare data collection. Explicit consent is required.	There are no rules and conditions for living in a (smart) city (*Slimme steden*, 2016).
Anonymity and pseudonymity	If you want to avoid explicit consent; anonymity (section 4.4.1) or pseudonymity (section 4.4.2) is required .	Being anonymous might not be feasible in smart cities. Data integration could lead to de-anonymization of one set of data (Narayanan and Shmatikov, 2008).
Proximity and locality	Using this concept, privacy is organized like living in a small village. Data can be collected whenever the owner is present (proximity) or when it is tied to a certain location (locality).	In this way it is difficult to integrate these data sources with others (Langheinrich, 2001), which might disable services in smart cities.
Adequate Security	Ideal would be to achieve authenticity and trusted communications.	Required power consumption and communication protocols don't always fit the object. For example chips in streetlights could be too small and not powerful enough to secure.
Access and recourse	Implement specific legal requirements, such as use limitation, access or repudiation.	Over-collecting is quickly done in smart cities (Li and Dai, 2016). Purposes might not be clear before data gathering.

4.4 Anonymity, pseudonyms and transparency

In this section we discuss anonymity, using pseudonyms, and transparency, since these concepts influence the impact on privacy as well as Smart City services. Below we will discuss the three paradigms and how they influence the tradeoff.

4.4.1 Anonymity

Anonymity is another way to control the flow of personal information. Anonymity has the aim to not expose the identity of a particular individual. Anonymity does not limit the ability to collect, analyze and use the data, nevertheless the data decreases in value. By anonymizing data, smart city services cannot be personalized per resident, which makes it impossible to recognize residents and discover personal patterns. Therefore anonymizing causes a loss of knowledge, which therefore reduces the benefits of the smart city services. Furthermore, anonymizing negatively affects accountability. Since no one can be hold accountable, anonymizing data facilitates misuse.

Nevertheless, in a non-profit environment, anonymity could contribute to offering services without being identified. Identification of individuals is not desirable for every service in a smart city environment. To identify general patterns, anonymity might be useful. Moreover residents might only give consent for relinquishing their data if it cannot be linked back to them.

4.4.2 Pseudonymity

Zarsky (2003) refers to pseudonymity as "the use of a 'virtual' personality or personalities by one physical individual when interacting in cyberspace or elsewhere" (p.1030). In this definition 'elsewhere' is an important aspect for the smart city, since the smart city concept vanishes the line between the virtual and the real world. Via pseudonyms the boundary of sharing information is thinner and gives the user more control on disclosing personal information since it protects one's identity.

Pseudonymity can either be traceable or untraceable (Froomkin, 1995). Untraceable pseudonymity makes use of an exclusive alias, which can not be traced back to the person by anyone in any way. The difference with anonymity is that there is some kind of identity, the pseudonym can create a personality on his own. The problem with untraceable pseudonyms is that a resident is hard to reach by other persons directly and privately. Therefore using untraceable pseudonyms is impractical for transactions which require two-way communication. Two-way communication is for example necessary when payments are involved. For most smart-city services untraceable pseudonyms therefore might not be applicable. Traceable pseudonymity allows a direct two-way link between the pseudonym and the physical person. A trusted third party (TTP) facilitates this connection. In this way it can accommodate interactions or business transactions. The advantage in comparison to an anonymous society is that persons are traceable, but still not identifiable. In this way the person who hides under a pseudonym can be a consistent personality. There are two challenges for having a sustainable society using pseudonyms: a trusted third party is essential, which causes security risks and relies on integrity; and when one person has multiple pseudonyms, for example for different services in a smart city, it should never be possible to link these pseudonyms (Zarsky, 2003).

4.4.3 Transparency

The term transparency implies openness, communication and accountability. A transparent smart city will monitor the city, but the residents will also have access to the gathered data and the way this data is used. In this way the collection of data is not limited, but the gathered data is open to everyone involved. Not only the governments and businesses have access to the data, but also the resident, from whom the data is mostly gathered. 'Knowledge is power', therefore transparency will balance the power between all involved parties. This is called a bottom-up approach, which enables residents to make their own decisions. Neirotti et al. (2014) concluded in their research that enabling every resident to access official documents in a simple way and to take part in the decision processes of a municipality will decrease the possibility for authorities of abusing the system for their own interests or hiding relevant information. Brin (1999), states that in a transparent society, participation and control will be valued over distrust and fatalism. Transparency has the aim to ensure equality. Important to note; data is not the same as information. Zarsky (2003) reasons that data mining tools are essential to fill the gap between data and information. Businesses mostly have more resources to develop the right data mining tools in comparison to residents. Concluding, open data is not enough to achieve the intended goals of transparency. Next, transparency does not fit in the currently used frameworks and laws, since it enhances data collection instead of limiting. Besides it increases the surveillance.

We can conclude that anonymity and pseudonymity can contribute to provide residents in the smart city with more control over the ownership of their data, by protecting residents to be identifiable by anonymizing data or using pseudonyms. Next, transparency improves the equality and balances the power between the businesses and the residents but induces many privacy risks.

Nevertheless, these principles might contradict to the business model of the smart city by decreasing the value of the data. When people decide on disclosing information for smart city services, it is important to know which paradigm is chosen since this influences risks and benefits.

4.5 Compensation

So far we discussed contractual norms to control the flow of information in smart cities, which contributes to protect residents' privacy. The earlier discussed CPM theory of Petronio (2012) stated that people make a risk/benefit analysis, when deciding on tradeoffs. Therefore the tradeoff might be influenced by compensations given for disclosing data, since this increases the benefits. In this section we will discuss the impact of compensations on the tradeoff.

4.5.1 Differences between users

A research of Hann et al. (2002) explored the trade-offs between three types of privacy concerns (errors, improper access and secondary use) and two types of benefits (monetary rewards and time savings) online consumers face when visiting a website. They confirm the presence of privacy calculus in individual decisions, showing that users are willing to give up some of their privacy for economic incentives.

Extending that study, (Hann et al., 2007) discover several clusters of users with similar utility patterns: privacy guardians, information sellers, and convenience seekers. Privacy guardians attach a relatively high value to information privacy. They value protection against error, improper access, and unauthorized secondary use of their personal information high by this group. Monetary rewards and visit frequency/time savings were valued relatively low by this group. Information sellers tend to sell their personal information relatively easy with little regard for convenience or privacy policies. Monetary rewards were valued high. Convenience seekers almost exclusively value convenience high (visit frequency/time savings). They are not concerned much with privacy policies or monetary rewards. Hann et al. (2007) argue that companies have the means to address the privacy concerns of their on-line consumers. They concluded that privacy policies are valued by users and that organizations may possess means to actively manage the privacy concerns of Internet users.

We can conclude from these studies that their might be differences among residents in valuating the tradeoff. Demographic questions might help understand these differences.

4.5.2 Construal Level Theory (CLT)

Another aspect which should be taken into account when looking at the risk/benefit ratio, is that benefits might be easier to oversee than risks. Issues regarding privacy could occur long after the tradeoff is made. The consequences of giving up privacy are hard to oversee for residents, following the Construal Level Theory (CLT) of Trope and Liberman (2010). CLT is a theory in social psychology that describes the relation between psychological distance and the extent to which people's thinking about objects and events, is abstract or concrete. According to CLT people perceive events that vary in several types of psychological distance: temporal, spatial, social or hypothetical distances. Regarding privacy, people could experience temporal and hypothetical distance. Privacy issues do not occur immediately when you share private or sensitive data. When disclosing one's data to a Smart City platform, it might not be clear for which purposes this data might be used. Hypothetical distance is about the likeliness of an event to happen. People mostly are aware of the privacy risks, but do not value them as very likely to happen. A compensation for disclosing data has a psychological short distance. Compensations might trigger people to disclose information, but this might not be the best thing to do in regard to peoples' privacy.

4.6 Social contract framework for smart cities

In this section we discuss the attributes regarding smart cities and present the conceptual Social contract framework for smart cities.

4.6.1 Attributes

The attributes chosen for the social contract framework for smart cities are based on the discussed literature by reviewing the properties of smart cities and the corresponding contractual norms. The dependent variable for this study is disclosing data and the independent attributes are: *compensation*, *sharing*, *specificity* and *storage*. We will discuss the chosen attributes below.

Compensation

Multiple privacy studies provide empirical evidence that compensating consumers for sharing their personal information can enhance their benefit perceptions of information disclosure (Phelps et al., 2000; Hui et al., 2007; Milne and Gordon, 1993). Hann et al. (2007) found that monetary rewards significantly affected individuals' preferences for websites with differing privacy policies.

These studies suggest that providing financial compensation constitutes an extra consumer outcome and an additional firm input, which is likely to increase the consumer's subjective judgments of the benefits of information disclosure. Concluding, people will sooner decide to disclose their information when monetary rewards are offered. The study of Milne and Gordon (1993), discussed at the beginning of this chapter, tested their Social contract framework via a conjoint study of trade-offs among all the attributes associated with direct e-mail (volume, targeting, compensation, and permission). It was found that the compensation factor (in terms of providing product discounts, gift certificates, and coupons) was the most important determinant of satisfaction.

Sharing

Distinctive for a smart city is the sharing of information with different kind of parties (Bhowmick et al., 2006). The CPM-theory (Petronio, 2012) suggests that people care about who becomes the co-owner of the information. In a smart city several businesses and authorities could create services with on the data stored at the smart city platform. Following the transparency theory of Zarsky (2003), when all information is open, everyone has the same information and the power in the city is balanced.

Storage

Another issue in the Smart City, where different parties cooperate, is which organization will store the collected information(Bhowmick et al., 2006). One of the principles of the CPM is about turbulences or regulation breakdowns. Co-owners of the data could be responsible for turbulences. Also the party who stores the information should have the same privacy rules as the consumer (Petronio, 2012). For example, the party should have adequate security and not sell the information if there is no consent.

Specificity

Last we make a distinction in the specificity of the data. In other words, if the data is collected real-time (every 10 seconds), every hour or every day. Depending on the level, the connected applications could perform real-time, semi-real time or not real time analysis and offer corresponding services. On the other side, when the data is more specific it is also more privacy sensitive.

4.6.2 Conceptual social contract framework

Based on the discussed and reviewed literature we drafted the following conceptual social contract framework for smart cities. The solid lines represent the exchange of information for smart city services. The bold lines represent the trade-offs residents and businesses and organizations consider before entering a social contract. The dotted lines represent communication channels. In comparison with the Social contract framework for e-mail marketing, one relation is added. Namely a direct communication channel between government and the smart city platform, since urban authorities are a direct stakeholder in smart city projects.

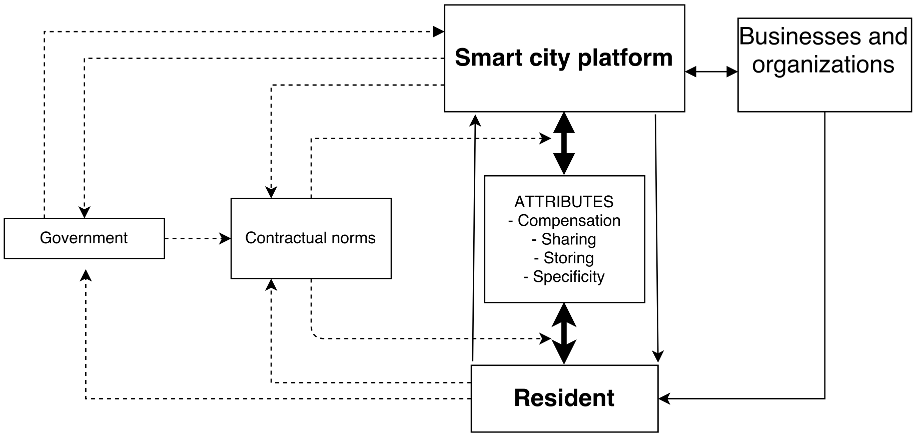


Figure 3: Conceptual social framework for smart cities

The purpose of the framework is to understand what different stakeholders of smart cities find important in the smart city tradeoff. The scope of this study is to research what residents find important in the smart city tradeoff, to provide recommendations and tools to urban authorities on how to govern residents interests in the smart city.
In Chapter 5, we discuss how we are going to research what residents find important in the smart city tradeoff, using the conceptual Social contract framework for smart cities.

5 Data and Methods

In this section we will discuss the research design, research methods and the final dataset.
First we discuss the research design. In order to empirically research what residents find important in smart city tradeoffs, we use Ruggedised as a context for the conceptual social framework for smart cities. The research consists of an online survey to study what people, from Hart van Zuid, find important when disclosing data to the Ruggedised project. An online survey was chosen to reach many people from Hart van Zuid to get an understanding of the residents' opinion on disclosing data to the smart city project. Moreover, it is the best way to conduct respond for conjoint analysis.
Next, we discuss the pilots, which contributed to the research design, and the sample of the research.
Second, the research method is choice-based conjoint(CBC) analysis to study what people find important in a smart city tradeoff. The CBC will be explained and we discuss why this is a suitable method to study the research objective.
Last we describe the final dataset.

5.1 Research design

This section elaborates on the research design of this study. We will discuss the questionnaire, which can broadly be divided into three parts: Choice-based conjoint, additional questions and demographics. These three parts are explained below.

Choice-based conjoint
The first part of the questionnaire incorporates the choice-based conjoint (CBC). Divided over multiple choice tasks, respondents are asked to indicate their preference given the displayed two smart meters. Considering the perceived difficulty of the service profiles and the estimated education level of the selected sample, respondents face only eight choice tasks, each comparing two alternatives to avoid noisy or biased results (Johnson and Orme, 1996). The results of the conjoint will show which attributes residents find more important than others and which levels per attribute are preferred above others.

All the attributes and their levels are presented in Table 3. The levels are chosen by applying the attributes of the conceptual Social contract framework for smart cities on Ruggedised. The levels of the attributes differ in degree of benefits as well as in risks.

Table 3: Attributes and levels

Attributes	Levels
Compensation *In exchange for sharing your data..*	there is no benefit. you get €20,- per year discount on your energy bill. you give €20,- per year to a sustainability project in Hart van Zuid.
Sharing *The data will be shared with..*	your energy provider. authorities connected to the smart city platform. everyone in the city, through an open smart city platform.
Storage *The data will be stored by..*	your energy provider. a trusted third party. the owner of the smart city platform (For example: The Municipality).
Specificity *The data will be updated every..*	10 seconds. hour. day.

Compensation can be given when residents decide to disclose data their smart meter data to the Smart city platform. Compensation contains three levels: no compensation, direct money or a donation to a common good. These levels are selected after an interview with two employees of the Innovation department of the Municipality of Rotterdam (Employee Municipality of Rotterdam, 2017).

The levels of *sharing* are: with your energy provider, with authorities connected to the smart city platform and with everyone in the city, through an open platform. The Energy provider would need the information for the smart grid. Other authorities can create other applications with the data. In an interview with the project manager of another smart city project in Rotterdam, the idea was mentioned to give everyone in the city access to the data (Project manager smart city, 2017). This would create a more transparent smart city, as (Brin, 1999) suggested.

In a conversation with the privacy officer of Eneco, a Dutch energy provider, it was made clear that he experienced that customers already expect that the energy provider stores their energy consumption data when using a Smart Meter. So far nobody had objected to this or asked to remove their data (Eneco Privacy Officer, 2017). *Storing* the data could also be done by the urban authority or a trusted third party (Chakrabarty and Engels, 2016).

Currently with consent of a group clients, Eneco stores real-time data from their special Smart Meter Toon. In this case the data is stored every 10 seconds (Eneco Privacy Officer, 2017). The other levels chosen for the *specificity* are per hour or per day, this decreases the value of the data but also increases the privacy of residents since they are not tracked every 10 seconds.

Additional questions disclosing data
The second part consists of additional questions to get a better understanding of why people would or wouldn't like to share their data. Since the conjoint analysis can only contain a few attributes and people are not able to exemplify their choices, additional questions can contribute to getting a better understanding of the choices that people make in the CBC part. The additional questions are particularly designed for the Ruggedised project and make a distinction between sharing personal data and anonymous data. Anonymous data is in the survey specified as 'data from which you cannot be identified'. This could either be by using pseudonyms or aggregating the data.
Questions are asked about for which purpose residents are prepared to share information and with who they are prepared to share information.

Demographics In the third part, respondents will be asked for several demographics, such as gender and nationality to conclude if the sample is representative for residents in The Netherlands.

5.1.1 Pilot

Several informal interviews have been conducted to set up the final research design. First of all a meeting with all stakeholders of the Ruggedised project was attended, to get an more extensive understanding of the project (Ruggedised Meeting, 2017).
The Municipality of Rotterdam employee responsible for the Hart van Zuid area, indicated that the average education level ranges from low to average in Hart van Zuid. Therefore in both the letter, which was send to the residents and the survey, the explanation of smart cities is simplified. An employee of the Research Business Intelligence department of the Municipality of Rotterdam contributed to setting up the letter to the residents of Hart van Zuid with the link to the survey.

The CBC questions were initially pilot under 49 students of a master program at the Erasmus University, Rotterdam. The purpose of the pilot was to see if the choice was understandable and if the attributes were clear. After discussing with several students it became clear that the attributes should be explained more and the levels of the compensation attribute, which were a certain percentage of discount on one's energy bill, were not very appealing and not concrete enough. In the final version of the survey these aspects have been adjusted.

5.1.2 Sample

The sample consists of residents of Hart van Zuid. To get the best understanding of the opinion of the residents of Hart van Zuid, all 1200 residents were invited to participate in the survey via a letter of the Municipality of Rotterdam. The letter contains a short description of the Ruggedised project and a link to the survey. The letter as well as the survey are in Dutch, and are presented in Appendix B and Appendix C.

In addition to the letter, a link to the survey was posted at the Facebook page 'Hart van Zuid Rotterdam'. The post addressed the residents of Hart van Zuid.

Besides residents of Hart van Zuid, residents from elsewhere were asked to participate in the survey, in order to analyze if there are significant population group differences. This would have consequences for the generalization of the research.
The other people were asked to participate by a Facebook post via the profile of the researcher. The post was open for public and was sharable.

Sample size

Following (Johnson and Orme, 1996), the formula for the size of the minimum sample size when performing CBC is:

$$\frac{nta}{c} >= 500$$

Where:
n = number of respondents
t = number of tasks
a = number of alternatives per task
c = number of “analysis cells"

When considering main-effects, c is equal to the largest number of levels for any one attribute. Since the survey considers all two-way interactions, c is equal to the largest product of levels of any two attributes. Respondents perform 8 tasks (textitt = 8), there are 2 alternatives per task (a = 2) and the number of analysis cells has a maximum of 3 (c = 3).

$$n \geq \frac{500 * 3}{8 * 2} \rightarrow n \geq 94$$

The number of respondents (n) is required to be at least 94.

5.2 Conjoint analysis

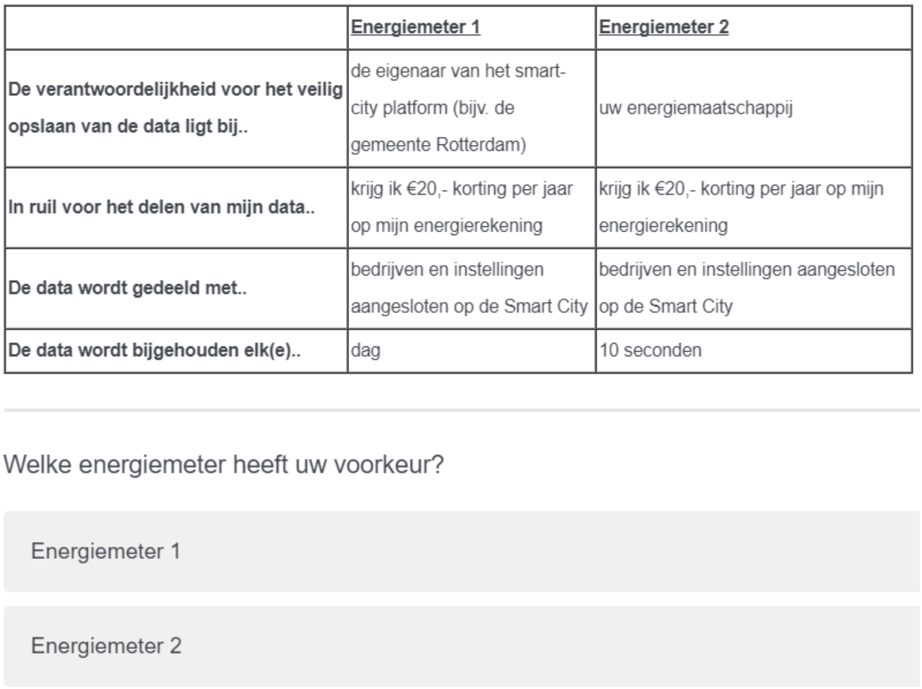
Decisions about privacy in smart cities involve a trade-off. Residents trade their information for smart city goods or services. To gain a clear understanding of how important each attributes is regarding the smart city tradeoff, we let respondents weight attributes of the tradeoff against each other in the survey.

Conjoint analysis is a decompositional method that estimates the structure of consumers' preferences. It estimates preferences given one's overall evaluations of a set of profiles that are pre-specified in terms of levels of different attributes (Green and Srinivasan, 1990). This trade-off can be decomposed into part-worth utilities and importance weights for each attribute of the service. In this way, the importance of different attributes or criteria in the consumer's evaluation of the service can be studied (Green et al., 1978). Following the Construal Level Theory of (Trope and Liberman, 2010), residents might not oversee the risks when it comes to disclosing information. Conjoint analysis makes residents carefully think about why the attributes induce risks, since they have to be balanced against other attributes that induce risks.

5.2.1 Choice-Based Conjoint (CBC)

Different conjoint methods exist. This research makes use of choice-based conjoint (CBC). CBC requires respondents to choose between two or more alternatives. As compared to ranking- or rating-based conjoint approaches, studies state CBC analysis to be more realistic in simulating consumer behavior (Natter and Feurstein, 2002) (Elrod et al., 1992). For CBC analysis the importance of each attribute is estimated based on a choice set. Every alternative can be described in terms of its attributes. The respondents are presented different alternatives, in this research two, and indicate which one they would actually choose. The advantage of CBC analysis is that the levels of the attributes can be randomly varied. In this way one can present multiple attributes with multiple levels and weight them against each other. A full factorial design is used to present the attributes. Collecting data with a full profile is realistic and preferred for situations in which there are fewer than six attributes (Green and

Srinivasan, 1990). In order to prevent biased results, the levels for each attribute are completely picked randomly, as well as the order in which the attributes appear for each respondent.
It is common to also include a ’None’-option next to the given alternatives. The ’None’-option is excluded from this research since the purpose of the research is to find out to what residents attach the most importance regarding attributes of the tradeoff, when they cooperate in the smart city they live in. An example of a choice task is presented in figure 4.



	Energiemeter 1	Energiemeter 2
De verantwoordelijkheid voor het veilig opslaan van de data ligt bij..	de eigenaar van het smart-city platform (bijv. de gemeente Rotterdam)	uw energiemaatschappij
In ruil voor het delen van mijn data..	krijg ik €20,- korting per jaar op mijn energierekening	krijg ik €20,- korting per jaar op mijn energierekening
De data wordt gedeeld met..	bedrijven en instellingen aangesloten op de Smart City	bedrijven en instellingen aangesloten op de Smart City
De data wordt bijgehouden elk(e)..	dag	10 seconden

Welke energiemeter heeft uw voorkeur?

Figure 4: Example choice-task

Nevertheless the choice-based conjoint method presents challenges. Respondents must process a lot of information when choosing a profile, since the respondents should make their decision based on all presented attributes. Therefore an implication of the CBC method is that only a limited number of attributes can be used. If too many attributes are included, respondents may base their preference only on a few attributes instead of all the shown attributes (Pullman et al., 1999). Green and Srinivasan (1990) recommend to not use more than six attributes in a full-profile conjoint. In this study we picked four attributes to avoid an overload of information. Next, following the "Number-of-Levels Effect" it matters if some attributes have more levels than others. Attributes defined on more levels tend to get more importance. It is recommended to choose about the same number of levels per attribute (Orme, 2002). Therefore in this research all the attributes contain three levels.

5.3 Data analysis

The data is analyzed in R. Conditional logistic regression and relative part-worth importances are used to analyze the choice-based conjoint tasks. In this section we will explain why this is a suitable analyzing method.

5.3.1 Conditional logistic regression

For analyzing the data we made use of conditional logistic regression. The conditional logistic regression model is introduced by McFadden (1973) and is based on a model similar to the logistic regression. The difference is that all individuals are subjected to different situations before expressing their choice. The fact that the same individuals respond to multiple choices, is taken into account by the conditional logistic regression model. In a standard regression, it is assumed that there is a linear relationship between variables. When applied on CBC data, this assumption would be violated since the choice variable is categorical (Energy meter 1 or Energy meter 2). Therefore the conditional logistic model expresses linear regression in logarithmic terms.
Conditional logistic regression is a form of semi-parametric inference, where complex relationships between unmeasured risk factors are controlled by organizing data into risk sets. This function fits and analyses conditional logistic models for binary outcome/response data with one or more predictors, where observations are not independent but are matched or grouped in some way.

The conditional logit model is based on a model similar to that of the logistic regression except that instead of having individual characteristics, there will be characteristics of the different alternatives proposed to the individuals.

The probability that individual i chooses product j is given by:

$$P_{ij} = e^{\beta^T z_{ij}} / \Sigma_k e^{\beta^T z_{ik}}$$

From this probability, we calculate a likelihood function:

$$l(\beta) = \Sigma_{i=1..n} \Sigma_{j=1..J}\ y_{ij} \log(P_{ij})$$

With y being a binary variable indicating the choice of individual *i* for product *j* and *J* being the number of choices available to each individual. To estimate the model parameters β (the coefficients of the linear function), it seeks to maximize the likelihood function (XLstat, 2017).

5.3.2 Relative Importance Attributes

Since the attributes are independent, we can calculate the relative importance given to each attribute. These relative importances are calculated with the *relaimpo* package of R (Grömping et al., 2006). The recommended metric is lmg (Harold and Lindeman, 1980).
The total relative importance per attribute is calculated by taking the mean of the relative importance given by each respondent. Since the importance is calculated per person, the logistic regression is not conditional. Therefore general logistic regression is applied in the function.

5.3.3 Data preparation

Several steps have to be taken before the data can be analyzed. R is used to prepare the data. First the data must be presented case by case; ungrouped, one subject/observation per row. this is different from the unconditional logistic function that accepts grouped or ungrouped data. Next, the binary outcome variable has to contain only 0 (control) or 1 (case). There must be a stratum indicator variable to denote the strata. In this way the choice cases can be grouped by participant and choice task.

5.4 Dataset description

In this section the dataset is described. The original dataset contained two separated parts, one with the results of the residents of Hart van Zuid and one with the residents from elsewhere. A total of 40 residents from Hart van Zuid replied to the survey and 134 residents from elsewhere. Results from respondents who did not complete the entire survey were excluded to ensure the reliability of the data (Fink and Litwin, 1995). After deleting the non-complete results 143 survey results were usable, 31 from Hart van Zuid and 112 from elsewhere. Via the letter which was spread under 1200 residents of Hart van zuid, 24 residents responded of which only 18 surveys were usable.

5.4.1 Characteristics respondents from Hart van Zuid

From Hart van Zuid 54% of the respondents is man and 46 % woman. Residents from all age categories responded, the most popular category being age 25 to 34 (35%). All of the respondents have the Dutch nationality. Half of the participants works full-time, the other half is fairly split in student, part-time work, unemployed and retired. More than half of the people have completed university of applied sciences (HBO) and 19 % only high school. 73 % of the respondents is unmarried.
77% of the respondents indicated that they already have a smart meter and 23% does not have one. The website of Hart van Zuid Rotterdam indicates that the residents of Hart van Zuid are multicultural young adults. The dataset does only contains Dutch respondents, which is therefore not totally representative.

5.4.2 Characteristics other respondents

From the other respondents, 56% is man and 44% woman. Most of the respondents are students (76%) in the age of 18-24 (74%). The other respondents are most of all working full-time (14%) or part-time (8%). Only 8,3% of the respondents is older than 35. This can be explained, since the survey was shared via the Facebook page of the researcher, being a 22 year old student.
All the respondents have the Dutch or German nationality. 67% of the respondents has completed a university degree, either a Bachelor or a Master. 16% has finished a HBO study and 14% finished only high school. 71% of the respondents is single.
In total, 23% of the respondents indicated to already have a smart meter. 67% indicated that they did not have one and the other 10% did not know if they have a smart meter or not.
Compared to the total population of residents in the Netherlands, respondents are a bit younger and higher educated. This should be taken into account when evaluating the results.

When comparing both groups we see that respondents from Hart van Zuid are older on average and have a slightly lower completed education level. The other group contains mostly students. Noticeable is that in Hart van Zuid roughly three-quarters of the respondents already has a smart meter, where from the other respondents only 23% is aware of having smart meter.
Since the response rate of the survey in Hart van Zuid was low, both datasets are combined to one dataset with an extra variable *hartvanzuid*. The value for the variable is 1 when a respondent lives in Hart van Zuid and 0 if not. The dataset will be referred to as 'total'.

In Chapter 6, we analyze the described final dataset with the discussed conditional logistic regression and we determine the part-worth importances for residents regarding the smart city tradeoff. Besides, we present the results of the additional questions.

6 Results

In this chapter we discuss the results of the survey. First we will present and discuss the results of the choice-based conjoint questions. Second we present the answers to the additional questions and we will discuss the outcomes.

6.1 CBC results

In this section we discuss the results of the CBC analysis. In Table 4 and 5 the results of the conjoint analysis are presented.

6.1.1 Effects attributes and levels

The four tested attributes; compensation, sharing, specificity and storage, with their corresponding levels and their effects on disclosing data for smart city services are presented in Table 4. We will discuss the implications per attribute.

Compensation
The attribute *Compensation* contains the levels 'no extra benefit', '€20,- goes to a sustainability project in the neighborhood' and 'I get €20,- discount on my energy bill'. The results show that there is a strong significant negative effect for no extra benefit when disclosing data ($-0.722, p < 0.001$) and a significant medium positive effect for getting €20,- discount on the energy bill ($0.260, p = 0.020$). This is in line with the studies discussed in Section 4.6.1, which stated that people are more prepared to disclose information when they are compensated.

Sharing
The attribute *Sharing* with levels 'companies and authorities connected to the Smart city platform', 'everyone in the city through an open online access to the Smart City' and 'your energy provider'. The results show that there is a strong negative effect on disclosing information with everyone in the city through an open online Smart City platform($0.796, p < 0.001$). In Section 4.4.3 we discussed the consequences of transparency for a Smart City (Brin, 1999). The results show that residents to not want to disclose their energy consumption data to everyone in their city. There is no significant difference between people who would prefer to share their energy consumption data with only their energy

Table 4: Conditional logistic regression table

	$coef$	$exp(coef)$	$se(coef)$	p
Compensation				
No extra benefit	-0.722	0.486	0.116	< 0.001
I get €20,- discount on my energy bill	0.260	1.297	0.111	0.020
Sharing				
Companies and authorities connected to the Smart city platform	0.091	1.096	0.114	0.422
Everyone in the city through an open online Smart City platform	-0.796	0.451	0.111	<0.001
Specificity				
Data per day	0.157	1.170	0.105	0.134
Data per hour	0.110	1.117	0.108	0.308
Storing				
A trusted third party	0.036	1.036	0.108	0.743
Your energy provider	-0.365	0.694	0.110	< 0.001

provider, and people who prefer to disclose their data to other companies connected to the Smart City platform.

Specificity
For the attribute *Specificity*, all the levels 'data per 10 seconds', 'data per hour' and 'data per day' do only cause small effects, which are not significant. Respondents therefore do not agree on a certain level of specificity and the results contain variance.

Storing
The attribute *storing* consists of the levels; 'your energy provider', 'a trusted third party' and 'the owner of the smart city platform'. Noticeable is the significant negative effect of storing of the data by one's energy provider(-0.365, $p < 0.001$). A trusted third party is slightly preferred above the owner of the Smart City platform (The Municipality in this case).

6.1.2 Relative Importances

In Table 5 the relative importances are presented for each attribute and the results are shown in Figure 5. The relative importances are calculated following the description in Section 5.3.2.

Table 5: Relative part-worth importances

	Mean Total (%)	Mean Hart van Zuid(%)	T-test (p-value)
Compensation	22.4%	23.2%	0.793
Sharing	31.6%	33.0%	0.740
Specificity	21.8%	17.0%	0.088
Storing	24.2%	21.3%	0.499

The results show that on average people give the most importance to sharing. When disclosing their energy consumption data to the smart city platform they are concerned that the co-owners, who are connected to the platform and obtain the data, do not have the same privacy rules. The results of the conditional logistic regression showed that people especially not want to disclose their data to everyone in the city. When combining the results residents are most concerned about their data being disclosed to everyone in the city. Sharing their data with everyone in the city would decrease their feeling of control over their data following the CPM theory (Petronio, 2008).

The second most relative importance on average is given to who is going to store the data of the smart city. This indicates that residents attach importance to who is responsible for storing the collected data. They prefer the data to be stored by the Municipality or a TTP over their energy provider. This can be explained by the privacy boundaries of the Municipality and a TTP being more similar to residents'. Moreover, concerns about turbulences, such as the data being hacked, can explain why residents find it more important that parties have the same privacy boundaries than the specificity of the data or the compensation they get.

The importance on average of compensation is third out of four. This differs from the research of Milne and Rohm (2000), who concluded that people give

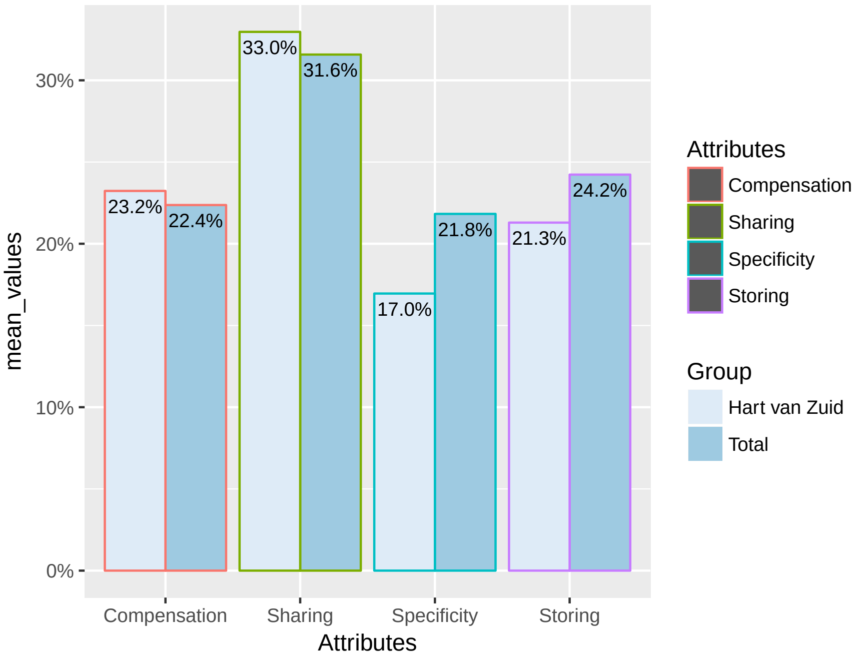


Figure 5: Average of the relative importances per attribute, given by respondents

the most importance to compensation in the tradeoff on e-mail marketing. The previous results of the regression showed that people prefer a compensation over no compensation, but they do find the compensation for disclosing their data more important than with who the data is shared and who stores the data.

Residents attach the least importance on average to the specificity of the data. Respondents also did not make a distinction between the different levels of the specificity attribute. Relatively to the other attributes respondents attached low importance to how specific the data is. This could indicate that if residents have the same privacy boundaries as the parties connected to the smart-city platform, they care less about what kind of data is shared.

When comparing the results from residents of Hart van Zuid with the total respondent group, there are small differences, but none of them are significant as is shown in Table 5. T-tests show no significant difference in respondents with a smart mater and without a smart meter. Also no significant differences were found between students and no students, see Appendix C.

In Figure 6, 7, 8 and 9 the distributions of the given importances by the respondents are shown in histograms per attribute. The black dashed line indicates the mean relative importance given, the grey dashed line indicates the median of the importance given to the attribute.

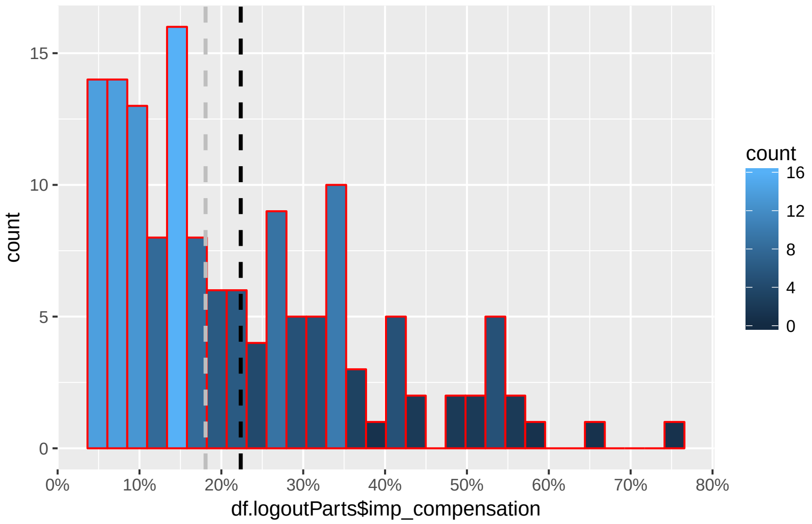


Figure 6: Relative importances given to compensation
($median = 0.181, mean = 0.224, st.deviation = 0.153$)

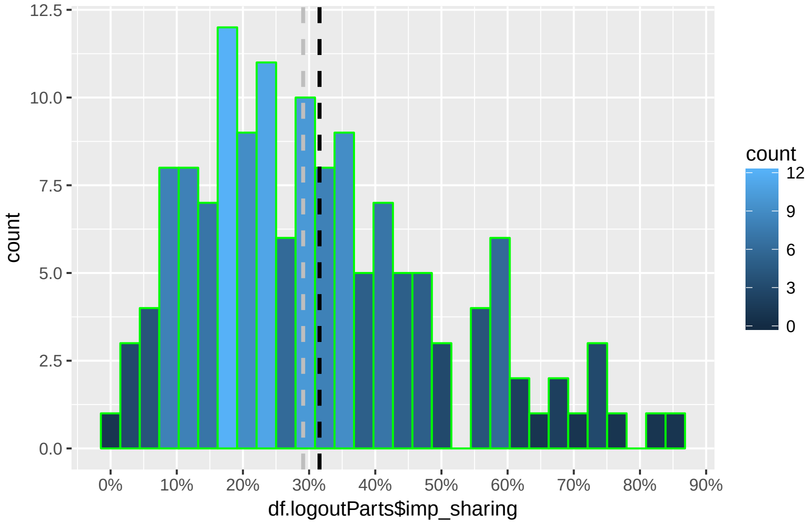


Figure 7: Relative importances given to sharing
($median = 0.291, mean = 0.316, st.deviation = 0.189$)

The histograms show that the opinions of residents are divided within an

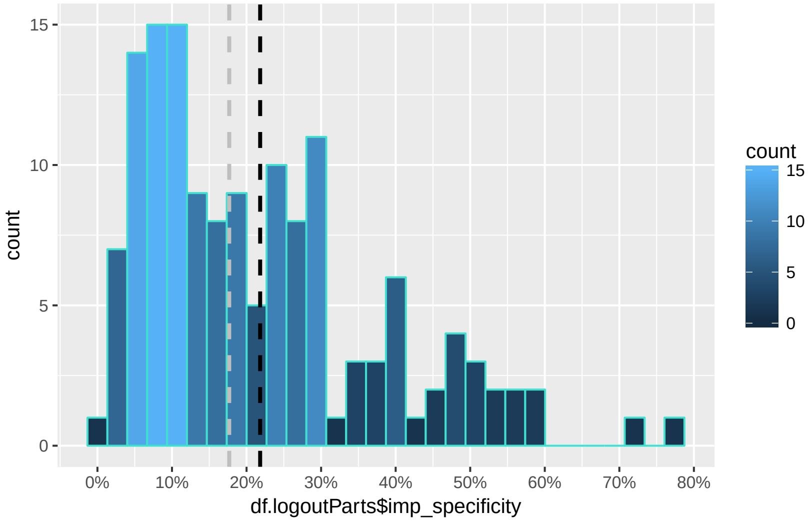


Figure 8: Relative importances given to specificity
($median = 0.177, mean = 0.218, std.deviation = 0.160$)

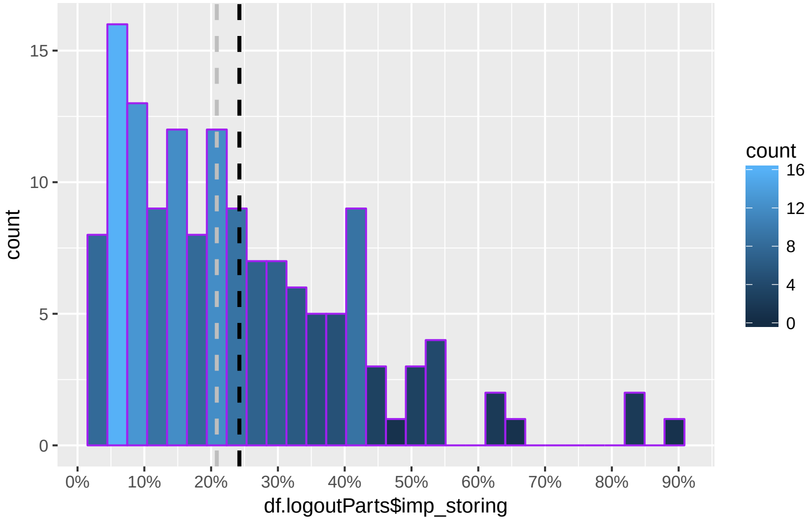


Figure 9: Relative importances given to storing
($median = 0.209, mean = 0.242, st.deviation = 0.174$)

attribute. For all the attributes the minimal value and maximum value are far apart. Where sharing and storing are somewhat normally distributed, the importances on contribution and compensation vary widely. This can be explained by the research of Hann et al. (2007), who stated that there are three different kind of users: Privacy guardians, information sellers and convenience seekers. Information sellers value compensations higher than other users and are therefore more likely to attach importance to compensation.

6.2 Results of the additional questions

In this section we discuss the additional questions of the questionnaire to get a better understanding of what residents find important in the tradeoff between disclosing energy consumption data and smart city services. We discuss for which purpose and with who, residents are prepared to disclose information about their energy consumption.

6.2.1 Purpose

In Table 6 and Figure 10 the results are presented of the question 'For which purposes would you be prepared to share data about your energy consumption?'. Respondents were allowed to choose multiple answers. The bars distinguish the two areas, and personal data and anonymous data.

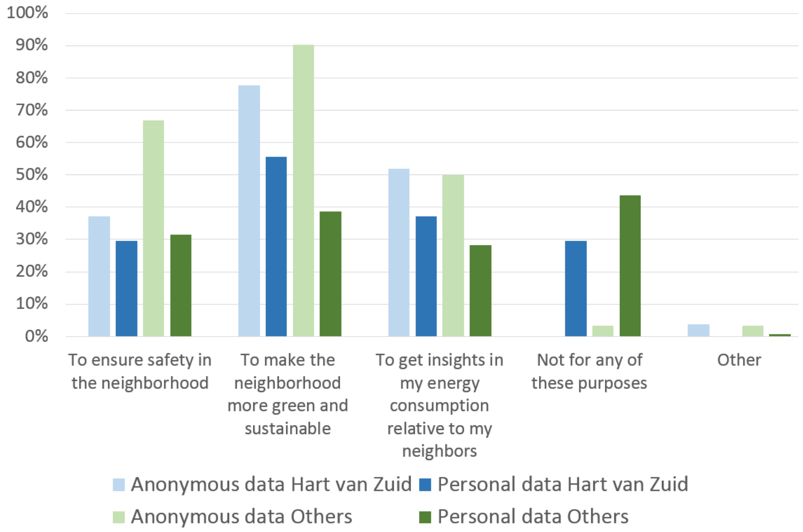


Figure 10: Purposes for which people are prepared to disclose their energy consumption data

First and foremost the results show that people make a distinction between

Table 6:
Purposes residents are prepared to disclose their energy consumption data for (in % of the total number of respondents)

Purpose	Anonymous data Hart van Zuid	Personal data Hart van Zuid	Anonymous data others	Personal data others
To ensure safety in the neighborhood	37%	30%	67%	31%
To make the neighborhood more green and sustainable	78%	56%	90%	39%
To get insights in my energy consumption relative to my neighbors	52%	37%	50%	28%
Not for any of these purposes	0%	30%	3%	44 %
Other	4%	0%	3%	1%

disclosing anonymous and personal data.
One can see that people are most willing to share data to make the neighborhood more green and sustainable. When the data is anonymous, almost everyone is prepared to disclose their information for this purpose. More or less half of the respondents is prepared to share anonymous data to get more insight in their energy consumption relative to their neighbors. Regarding the personal data, a quarter to half of the respondents is not prepared to share their data for the mentioned purposes in the question.

6.2.2 Co-owners

Petronio (2012) states in her research that people are prepared to share their information with others if they believe these co-owners have the same rules and boundaries. Since respondents do not know for which purpose the data will be used exactly, the question focuses more on who people trust to have the same boundaries. In Table 7 and Figure 11 the results are presented on the multiple-choice question (where it was allowed to choose more options) 'With whom are you prepared to share your data about your energy consumption?'.

Table 7:
Parties residents are prepared to disclose their energy consumption data to

Purpose	Anonymous data Hart van Zuid	Personal data Hart van Zuid	Anonymous data Others	Personal data others
Police	41%	75%	37%	45%
Fire brigade	41%	77%	33%	51%
The Municipality	59%	59%	41%	49%
Neighbourhood residents	41%	48%	15%	7%
Students	19%	52%	7%	9%
Start-ups	15%	40%	4%	9%
Companies	15%	40%	4%	9%
Nobody	15%	5%	37%	37%
Other	7%	5%	4%	2%

The results show that the respondents again distinguish anonymous and personal data. Most respondents are prepared to disclose their data to the police, fire brigade and the Municipality. Almost 40% of the respondents indicates not being prepared to share their personal data with anybody.

6.2.3 Open question

In the survey one open question was included: "Why would you or would you not be prepared to disclose your data on energy consumption?". The answers give an exploratory insight in what people are thinking about the topic. Almost everyone answered the question, while this was optional. Participants showed to be interested in the topic and gave comprehensive answers, showing knowledge and (strong) opinions. For example, one participant stated:
'I would be prepared to share my energy consumption, since collecting these data of

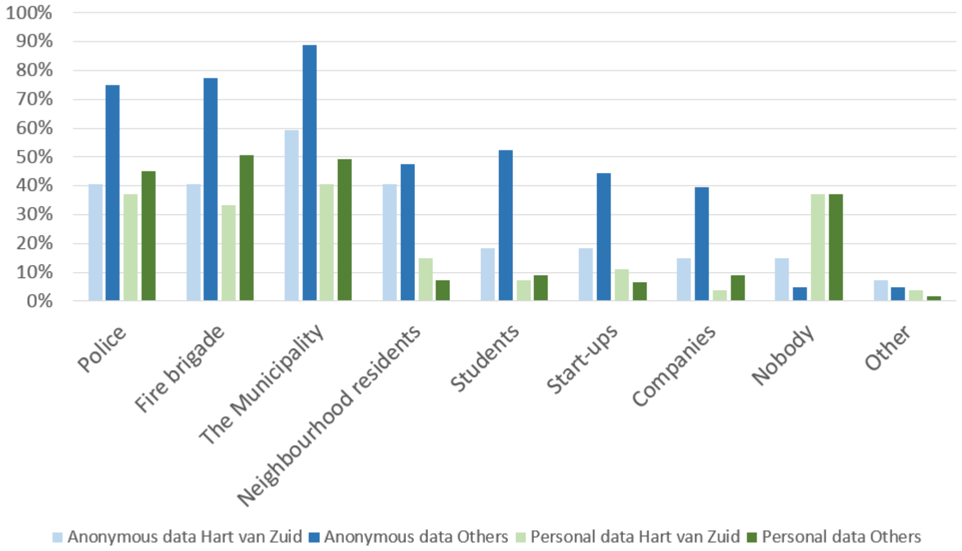


Figure 11: Parties residents are prepared to disclose their energy consumption data to

households in a neighborhood could help a project, like the smart city, to better divide energy and thereby prevent an oversupply. I think wisely handling energy is more important than not sharing data about my energy consumption - assuming this is all done in a safe environment.'.

A summary of the given answers is presented in Table 8

Many of the possible risks of smart meters stated by McKenna et al. (2012) are mentioned in the comments as a reason why they are not prepared to share their energy consumption data. Next, the participants explain that they do not want to share data every 10 seconds (specificity), since it makes it possible to track everything you do at that moment. They are most afraid for misuse of the data by burglars, for being able to know when they are home. This counters the results of the CBC, which stated that people do not care about the specificity of the data and give the least importance to this. The difference in results might be caused by the difficulty of overseeing the consequences of the different levels of the attribute by every participant. This would confirm the CLT which states that people give less importance to attributes of which the risks are less visible or tangible (Trope and Liberman, 2010). Next, participants are afraid that the data will not be handled in the right way and companies do not have the same privacy boundaries. They indicate that often their consent is not handled in the right way. The GDPR, the new European privacy might mitigate in this concern as explained in Section 4.3.

Table 8: Summary of open answers on *"Why would you or would you not be prepared to disclose your data on energy consumption?"*

	Reasoning
Prepared	Getting more insight in personal energy consumption. Helping the environment by reducing energy consumption. Getting financial benefits for disclosing data. Not attaching value to the data.
Not Prepared	It is readable from the data if one is home or not, which can be misused. Do not see the purpose of sharing the information with everyone in the city. It is nobody's business.

On the other side, respondents do acknowledge the increased value of collecting data on a smart city platform. Many participants indicate that they are prepared to share their data if it helps the environment. Participants thoughts on the topic confirm the literature, which states that more awareness of energy consumption can lead to reducing consumption (Owen and Ward, 2006). Next the participants have a positive attitude to smart grids.

7 Assumptions and conclusions

In this chapter we review the main findings of this study and discuss these findings, to answer the research question: *'What do residents find important in the tradeoff between disclosing data and smart city services'*. Next, we discuss the managerial implications to give recommendations and tools to urban authorities. Last, we discuss the limitations and further research.

7.1 Main findings

The research question of what residents find important in the smart city tradeoff is attempted to be answered by this exploratory survey. In this section we review the main findings of the study.

To answer the research question we drafted a Social contract framework for smart cities, with four attributes chosen based on literature on smart cities: *compensation*, *sharing*, *specificity* and *storage*. The attributes are tested via choice-based conjoint analysis, to establish relative importances given by residents. We discuss the findings on the four attributes in order of the average relative importance of the residents for the smart city tradeoff: *sharing*, *storage*, *compensation* and *specificity*. Nevertheless, the results show that the relative importances given to each attribute differs per resident.

Sharing
Residents attach the most importance to with who the data is shared. With who the data is shared has an effect on the decision to disclose data by residents.
One of the conclusions that can be derived from *sharing* is: residents prefer not to disclose their energy consumption data to everyone in the city. A strong negative effect was found on disclosing energy consumption data with everyone in the city. The comments on the open question made clear that several people do not see why this would be relevant. The results also show that people are prepared to share the information with many parties and several purposes, when the data is aggregated or anonymous. This decreases the risks people attach to sharing data. However in the literature section we have concluded that in a smart city it will be hard to keep data anonymous, when data from multiple sources is combined. Another interesting finding is that many residents indicated to want more insight in their data. If they disclose data to the smart city platform residents indicate they want insight in their own data. Many residents indicated that they are prepared to share their energy consumption data with their neighbors in a way that they get more insights in their consumption and

to compare their consumption with similar households in the neighborhood if this is done anonymously.

Storing
Residents prefer the Municipality and a Trusted Third Party over their energy provider to store their data. The results show that people do not distinguish the Municipality and a TTP for storing their energy consumption data. The CPM theory (Petronio, 2008) explains this by residents having different privacy boundaries than their Energy provider and concerns of turbulences, for example misuse of the data.

Compensation
Residents prefer a personal benefit. This is picked over supporting a local sustainability project and not receiving any compensation. People are sooner prepared to disclose their information to parties when they retrieve a compensation in return.

Specificity
Regarding the specificity of the data, the preferred way of disclosing differs a lot per person. Some see great risks lying in sharing specific data, were others see none. The results on the open question show, contradicting to the CBC, that people foresee privacy risks in others being able to track them every 10 seconds.

Besides, the results of the additional questions showed that people distinguish personal and anonymous data when they decide on purposes and parties to disclose their energy consumption data to. Next, the open questions showed that residents are informed about the topic of disclosing energy consumption data for services and do have concerns regarding their privacy when their data is disclosed.

7.2 Discussion

In this section we evaluate the conceptual Social contract framework for smart cities, using the main findings of the study. Then we answer the research question and discuss the remarks.

When we place the main findings in our conceptual Social contract framework for smart cities, we find that the differences between residents on what they find important in the tradeoff regarding smart cities can be explained by the contractual norms of the residents (Milne and Gordon, 1993). Besides, we find that some of the picked attributes might be more suitable for the framework than others. We will discuss these conclusions below.

First, following the Social contract framework the differences between residents can be explained by different having different contractual norms. In Section 4.2 the CPM theory was discussed. The theory states that residents' personal privacy boundaries depend on five principles: Ownership, control, co-ownership, privacy rules, and turbulences and regulation breakdowns. Personal privacy rules and boundaries can explain the differences in what people find important when they disclose data to smart cities.
Moreover, as (Milne and Gordon, 1993) stated, variance could also be explained by difference in salience of people of the legal norms on privacy. The smart city challenges the current privacy laws and therefore residents might be concerned they are not protected by the current laws (Langheinrich, 2001). This concern might change when the GDPR, the new European privacy law, is enforced.
However, the results of the do not explain which norms explain the differences, to find out further research is necessary.

Second, we evaluate the attributes chosen for the smart city tradeoff: compensation, sharing, storing and specificity. Sharing and storing of the disclosed information turned out to be relatively the most important. This confirms the theory of Petronio (2008), which states that people attach importance to the privacy boundaries of the co-owners of the information. Significant distinguishes are made between the different levels of the attributes. Both sharing and storing were somewhat normally distributed, which supports taking the average importance of residents.
The data about compensation is not normally distributed, which is supported by the theory of Hann et al. (2007). Their research found that there are three different kinds of users: Privacy guardians, information sellers and convenience seekers. Information sellers value compensations higher than other users and are therefore more likely to attach importance to compensation.
Specificity seems to be a difficult attribute for people to estimate, since there where no differences found in the conjoint analysis between the levels, but in the open question people indicated they are concerned about data obtained every 10 seconds.

By evaluating the social contract framework for smart cities, we conclude that the framework can be applied on smart cities to gain understanding on what residents find important in the smart city tradeoff, but further research has to explore other attributes concerned with the tradeoff. We discuss this more extensively in Section 7.4.

With the evaluated conceptual framework, we will now answer the research question: *What do residents find important in the tradeoff between disclosing data and smart city services?* We conclude that residents find it relatively important with who the data is shared and by who the data is stored in the smart city tradeoff. This implicates that residents attach relative importance to who become the co-owners of the data when they disclose their data to the smart city platform. Another conclusion is that residents attach less importance to the compensation they get for disclosing their data and how often the data is disclosed. However, residents do distinguish personal and anonymous data, which implicates that residents also attach importance to how personal the data is.

Nevertheless, remarks have to be made on the context in which the research question is studied. Since the Ruggedised project was used as the context, the survey was on disclosing energy consumption data to the smart city platform of Ruggedised. Therefore the results are specified on smart city projects which collect energy consumption data, for example smart grid projects (Owen and Ward, 2006). With the Social contract framework for smart cities, other contexts can be researched to find out if there are significant differences in what kind of data is shared on what residents find important in the smart city tradeoff.
Since there were no significant differences in the results between Hart van Zuid and residents from elsewhere, it can be derived that results are not influenced by the research being about a concrete smart city project in the area of the respondents. Therefore the conclusions can be used for smart city projects outside Hart van Zuid.
As a last remark, only four attributes have been tested in the conjoint analysis. Therefore we can not conclude that these are the most importance attributes for residents, but only which attribute gets relatively more importance than the other researched attributes.

7.3 Managerial implications

This chapter will elaborate on recommendations and tools for urban authorities.
The recommendations and tools can help urban authorities to draft policies for smart city projects in regard to residents privacy. This steps in on the concerns stated by the report of Kool et al. (2017), stating that society is not yet ready for the digitization. Urban authorities should take their responsibility in protecting residents' privacy in smart city projects. Urban authorities can give residents more voice in smart city projects, where businesses might have opposing interests regarding the tradeoff.

Give high importance to with who the data will be shared
In order to increase residents' disclosing of data, high importance should be given to who will be connected to the smart city platform. This research found that people distinguish the kind of parties they want to share their data with.

Therefore it is useful to inform people with which parties the data will be shared and what their contractual norms are. In this way people can make an informed decision on disclosing their data in exchange for smart city services.

Residents are positive on sharing data for sustainability

Next this research found that people are positive on sharing their data to make the neighborhood more green and sustainable. Therefore it is recommended to research possibilities of letting residents participate in smart grid projects. In this way residents do not only live in the smart city but are also involved and cooperate. If the data is collected anyways for smart grid projects it is interesting to research opportunities to give the residents more insight in their energy consumption. The study indicated that many residents would prefer to get more insight in their energy consumption, to become more aware of their energy consumption. Residents believe that this could lower their energy consumption. Since it is also a goal of the government to reduce energy consumption, urban authorities might jump in on this demand.

Distinguish Anonymous and Personal data

The research shows that residents make a distinction between sharing anonymous data and personal data. They are prepared to share anonymous data (data from which they can not be identified) for more purposes and with more parties. We therefore recommend to investigate for which purposes anonymous data is sufficient and for which purposes personal data is needed. In this way people might be more willing to disclose their data.

Take into account residents' privacy awareness

This research found that residents are aware of the privacy risks of sharing data to smart city platforms. Residents showed to be informed. Multiple privacy concerns were indicated by residents in regard to disclosing their data to the smart city platform. Therefore we recommend to not ignore residents' concerns, since this could cause obstacles. As a solution privacy concerns of residents should be investigated to research what causes them and if they can be mitigated. For example, if residents are concerned because they are feeling that they have no common privacy boundaries or are not aware of certain laws which protect their privacy, residents can be further informed.

Do not focus on compensation

The last recommendation is to not focus on giving compensations to residents for disclosing their data to smart city platforms. Residents do relatively not attach much importance to the compensation. Next, it persuades residents to disclose information, which might induces residents' privacy risks.

7.4 Limitations & further research

In this Section we discuss the limitations and discuss further research.

Sample
Residents from Hart van Zuid were chosen as sample for the study. As stated before from all 1200 residents of the neighborhood who were invited to participate via a letter in their mailbox, only 24 residents responded to the survey of which 18 surveys were complete. A non-response rate of 98% is high and limits the research, since the respondents group might be biased. respondents might have known more about or been more interested in, the topic or the Ruggedised project.
Since the letters were posted in the mailbox and no personal contact was made with the invited residents, it is unclear why the response rate was this low. It could be caused by people did not read their mail in the two weeks the survey was set out. Another reason could be people did not want to take the effort to start the survey on their computer while the (shortened) link was on paper. Another reason could be that people could not read Dutch, the area is highly multi-cultural. There were no resources to adjust the language for every household. Also the questionnaire was spread from the Municipality of Rotterdam, this was indicated on the envelop and in the letter. Perhaps people distrusted this. Furthermore, people might not have been interested enough in the topic. The letter made clear that the survey was about data sharing with a smart city project in their neighborhood. Perhaps people did not understand the concept of smart cities and therefore did not respond or did not complete the survey. Further research is needed to find out what was the cause of the low responds. This can contribute to research on how residents can be involved in the decision process on complex urban topics regarding residents.

Context
Ruggedised was chosen to set a context. The advantage of choosing the project is that the context was clear and the example was real-life. As a consequence the basis of the study was designed for the project. Since energy consumption data was chosen as the information to disclose to the smart city, the study might be biased on this kind of data. Therefore we can not say the conclusions of the study are applicable for any kind of data. Further research is needed to find out if the importance of attributes are dependent on the kind of data disclosed to the smart city platform.

Additional questions
The additional questions are not academically tested and therefore not reliable

for academic conclusions. Nevertheless it does explore residents opinions and supported the CBC part. Further research is needed to gain academic insights in these topics.

Social contract framework for smart cities

The purpose of the framework is to understand what different parties find important in the smart city tradeoff. The scope of this research is what residents find important in the tradeoff, to provide recommendations to urban authorities on how to govern residents' privacy in the smart city. This research implicated that there is variance between residents. To better understand the variances between residents, further research is needed, to gain knowledge on where privacy concerns of residents could be mitigated regarding the differences in contractual norms. This could be researched by other methods. For example, interviews and focus groups with residents to deeper discuss why or why not residents would disclose their data to the smart city platform. It could elaborate on the results found in this study that people do not prefer to disclose information with everyone, and look for explanations.

Next, the contractual norms and laws will change in the upcoming years. People's view on privacy and their personal privacy boundaries could change. Therefore it is interesting to research residents decisions on disclosing information over time and see if there is a change which might impact society.

Last, in order for the government to draft policies, the stakes of all parties presented in the framework should be researched. Then the government can consider the stakes of all stakeholders and draw policies on the smart city tradeoff.

Bibliography

Bhowmick, S. S., Gruenwald, L., Iwaihara, M. and Chatvichienchai, S. (2006). Private-iye: A framework for privacy preserving data integration, *Data Engineering Workshops, 2006. Proceedings. 22nd International Conference on*, IEEE, pp. 91–91.

Brin, D. (1999). *The transparent society: Will technology force us to choose between privacy and freedom?*, Basic Books.

Caragliu, A., Del Bo, C. and Nijkamp, P. (2011). Smart cities in Europe, *Journal of Urban Technology* **18**(2): 65–82.

Chakrabarty, S. and Engels, D. W. (2016). A secure IoT architecture for smart cities, *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, IEEE, pp. 812–813.

Darby, S. et al. (2006). The effectiveness of feedback on energy consumption, *A Review for DEFRA of the Literature on Metering, Billing and direct Displays* **486**(2006).

Durham, W. T. (2008). The rules-based process of revealing/concealing the family planning decisions of voluntarily child-free couples: A communication privacy management perspective, *Communication Studies* **59**(2): 132–147.

Elrod, T., Louviere, J. J. and Davey, K. S. (1992). An empirical comparison of ratings-based and choice-based conjoint models, *JMR, Journal of Marketing Research* **29**(3): 368.

Employee Municipality of Rotterdam, G. (2017). Innovation department, personal communication (07-06).

Eneco Privacy Officer, R. (2017). personal communication (22-05).

Fink, A. and Litwin, M. S. (1995). *How to measure survey reliability and validity*, Vol. 7, Sage.

Froomkin, A. M. (1995). Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases, *Journal of Law and Commerce* **15**: 395.

Green, P. E., Rao, V. R. and DeSarbo, W. S. (1978). Incorporating group-level similarity judgments in conjoint analysis, *Journal of Consumer Research* **5**(3): 187–193.

Green, P. E. and Srinivasan, V. (1990). Conjoint analysis in marketing: new developments with implications for research and practice, *The Journal of Marketing* pp. 3–19.

Grömping, U. et al. (2006). Relative importance for linear regression in R: The package 'relaimpo', *Journal of Statistical Software* **17**(1): 1–27.

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

Hann, I.-H., Hui, K.-L., Lee, T. and Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off, *ICIS 2002 Proceedings* p. 1.

Harold, R. and Lindeman (1980). Introduction to bivariate and multivariate analysis, *Technical report*.

Heide, J. B. and John, G. (1992). Do norms matter in marketing relationships?, *The Journal of Marketing* pp. 32–44.

Hui, K.-L., Teo, H. H. and Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory field experiment, *Mis Quarterly* pp. 19–33.

Johnson, R. M. and Orme, B. K. (1996). How many questions should you ask in choice-based conjoint studies, *Art Forum, Beaver Creek*.

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

Kool, T., Royakkers and van Est (2017). Opwaarderen - borgen van publieke waarden in de digitale samenleving (https://www.rathenau.nl/nl/publicatie/opwaarderen-borgen-van-publieke-waarden-de-digitale-samenleving).

Langheinrich, M. (2001). Privacy by design — principles of privacy-aware ubiquitous systems, *International conference on Ubiquitous Computing*, Springer, pp. 273–291.

MacDonald, M. (2007). Appraisal of costs & benefits of smart meter roll out options, *Final Report. Report for Department of Business Enterprise and Regulatory Reform, London.* **17**: 08–11.

McKenna, E., Richardson, I. and Thomson, M. (2012). Smart meter data: Balancing consumer privacy concerns with legitimate applications, *Energy Policy* **41**: 807–814.

Metzger, M. J. (2007). Communication privacy management in electronic commerce, *Journal of Computer-Mediated Communication* **12**(2): 335–361.

Milne, G. R. and Gordon, M. E. (1993). Direct mail privacy-efficiency tradeoffs within an implied social contract framework, *Journal of Public Policy & Marketing* pp. 206–215.

Milne, G. R. and Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives, *Journal of Public Policy & Marketing* **19**(2): 238–249.

Mohsenian-Rad, A.-H., Wong, V. W., Jatskevich, J., Schober, R. and Leon-Garcia, A. (2010). Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid, *IEEE Transactions on Smart Grid* **1**(3): 320–331.

Murphy, M. H. (2015). The introduction of smart meters in ireland: Privacy implications and the role of privacy by design.

Narayanan, A. and Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets, *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, IEEE, pp. 111–125.

Natter, M. and Feurstein, M. (2002). Real world performance of choice-based conjoint models, *European Journal of Operational Research* **137**(2): 448–458.

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G. and Scorrano, F. (2014). Current trends in smart city initiatives: Some stylised facts, *Cities* **38**: 25–36.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*, Stanford University Press.

Orme, B. (2002). Formulating attributes and levels in conjoint analysis, *Sawtooth Software research paper* pp. 1–4.

Owen, G. and Ward, J. (2006). Smart meters: commercial, policy and regulatory drivers, *Sustainability First* p. 54.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples, *Communication Theory* **1**(4): 311–335.

Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by, *Journal of Family Communication* **4**(3-4): 193–207.

Petronio, S. (2008). *Communication privacy management*, Wiley Online Library.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation?, *Journal of Family Theory & Review* **2**(3): 175–196.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*, Suny Press.

Petronio, S. and Altman, I. (2002). Boundaries of privacy.

Phelps, J., Nowak, G. and Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information, *Journal of Public Policy & Marketing* **19**(1): 27–41.

Project manager smart city, R. (2017). personal communication (15-05).

Pullman, M. E., Dodson, K. J. and Moore, W. L. (1999). A comparison of conjoint methods when there are many attributes, *Marketing Letters* **10**(2): 125–138.

Ramirez, E. (2013). *The privacy challenges of big data: a view from the lifeguard's chair*, US FTC.

Regulation, G. D. P. (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46, *Official Journal of the European Union (OJ)* **59**: 1–88.

Rogai, S. (2006). Enel's metering system and telegestore project, *NARUC Conference*.

Ruggedised (2016). Ruggedised report, *Retrieved via the Municipality of Rotterdam* .

Ruggedised Meeting, S. (2017). Meeting (15-02).

Sanchez, L., Galache, J. A., Gutierrez, V., Hernandez, J. M., Bernat, J., Gluhak, A. and Garcia, T. (2011). Smartsantander: The meeting point between future internet research and experimentation and the smart cities, *Future Network & Mobile Summit (FutureNetw), 2011*, IEEE, pp. 1–8.

Slimme steden (2016). Tegenlicht.
URL: *http://www.npo.nl/vpro-tegenlicht/01-05-2016/*

Stanton, J. M. and Stam, K. R. (2002). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives, *Surveillance & Society* **1**(2): 152–190.

Strandburg, K. J. (2014). Monitoring, datafication and consent: legal approaches to privacy in the big data context, *Privacy, big data and the public good (eds Lane J, Stodden V, Bender S, Nissenbaum H)* pp. 5–43.

Strbac, G., Gan, C. K., Aunedi, M., Stanojevic, V., Djapic, P., Dejvises, J., Mancarella, P., Hawkes, A., Pudjianto, D., Le Vine, S. et al. (2010). Benefits of advanced smart metering for demand response based control of distribution networks, *ENA/SEDG/Imperial College report on Benefits of Advanced Smart Metering (Version 2.0) Energy Networks Association, London, 2010* .

Thompson, J., Petronio, S. and Braithwaite, D. O. (2012). An examination of privacy rules for academic advisors and college student-athletes: A communication privacy management perspective, *Communication Studies* **63**(1): 54–76.

Trope, Y. and Liberman, N. (2010). Construal-level theory of psychological distance, *Psychological Review* **117**(2): 440.

United-States-Federal-Trade-Commission (1998). *Privacy online: a report to Congress*, The Commission.

Warren, S. D. and Brandeis, L. D. (1890). The right to privacy, *Harvard Law Review* pp. 193–220.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R. A., Hayes, N. and Nelson, L. E. (2009). Helping CIOs understand "smart city" initiatives, *Growth* **17**(2): 1–17.

Weiser, M. (1991). The computer for the 21st century, *Scientific American* **265**(3): 94–104.

West, R. and Turner, L. H. (2013). Introducing communication theory: Analysis and application (2013 ed.).

Westin, A. (1967). In privacy and freedom, *New York: Atheneum* p. 7.

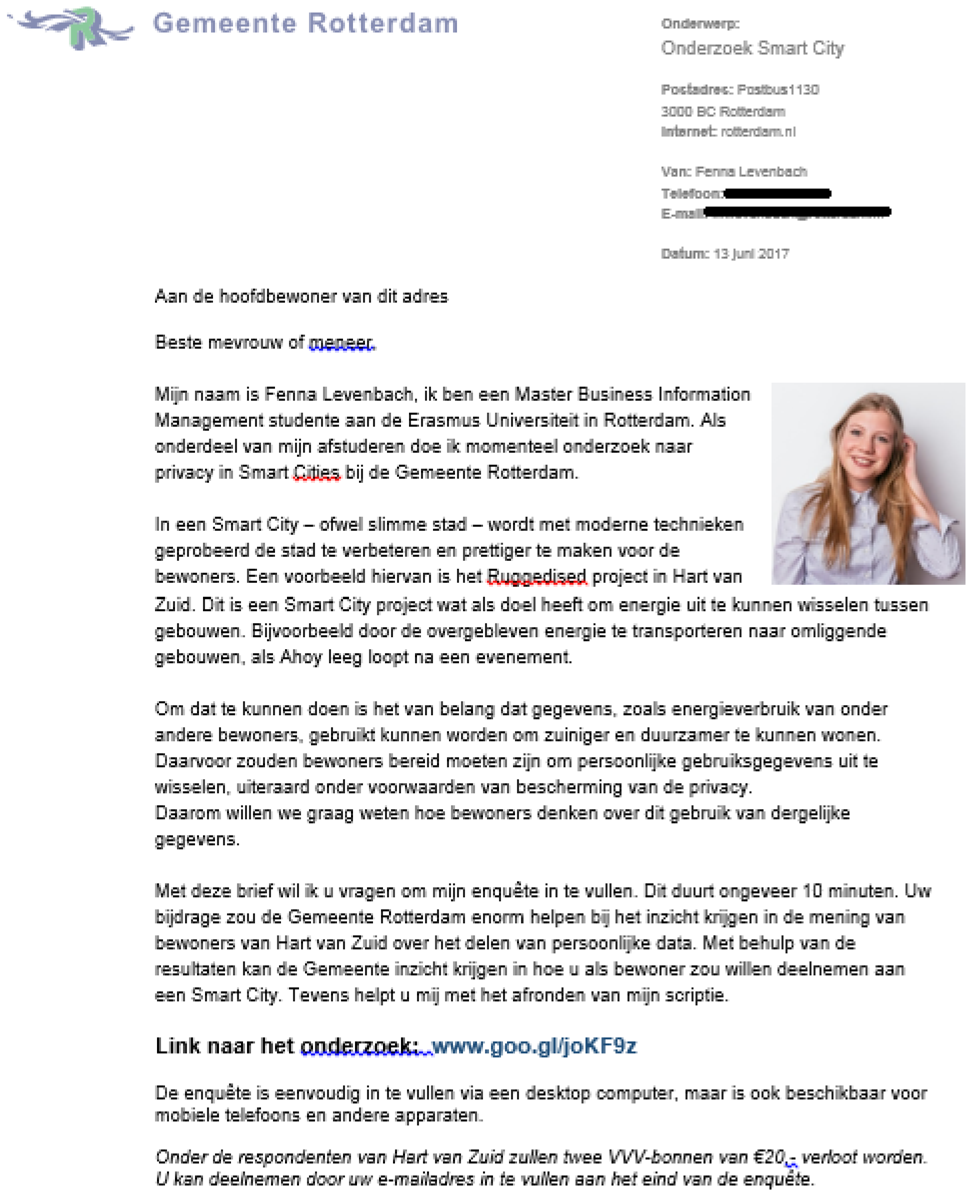
Westin, A. F. (1968). Privacy and freedom, *Washington and Lee Law Review* **25**(1): 166.

XLstat (2017). Conditional logit model. Accessed: 2017-07-03.
URL: *https://www.xlstat.com/en/solutions/features/conditional-logit-model*

Zarsky, T. Z. (2003). Thinking outside the box: Considering transparency, anonymity, and pseudonymity as overall solutions to the problems in information privacy in the internet society, *University of Miami Law Review* **58**: 991.

Appendices

Appendix A



Gemeente Rotterdam

Onderwerp:
Onderzoek Smart City

Postadres: Postbus1130
3000 BC Rotterdam
Internet: rotterdam.nl

Van: Fenna Levenbach
Telefoon: [redacted]
E-mail [redacted]

Datum: 13 juni 2017

Aan de hoofdbewoner van dit adres

Beste mevrouw of meneer,

Mijn naam is Fenna Levenbach, ik ben een Master Business Information Management studente aan de Erasmus Universiteit in Rotterdam. Als onderdeel van mijn afstuderen doe ik momenteel onderzoek naar privacy in Smart Cities bij de Gemeente Rotterdam.

In een Smart City – ofwel slimme stad – wordt met moderne technieken geprobeerd de stad te verbeteren en prettiger te maken voor de bewoners. Een voorbeeld hiervan is het Ruggedised project in Hart van Zuid. Dit is een Smart City project wat als doel heeft om energie uit te kunnen wisselen tussen gebouwen. Bijvoorbeeld door de overgebleven energie te transporteren naar omliggende gebouwen, als Ahoy leeg loopt na een evenement.

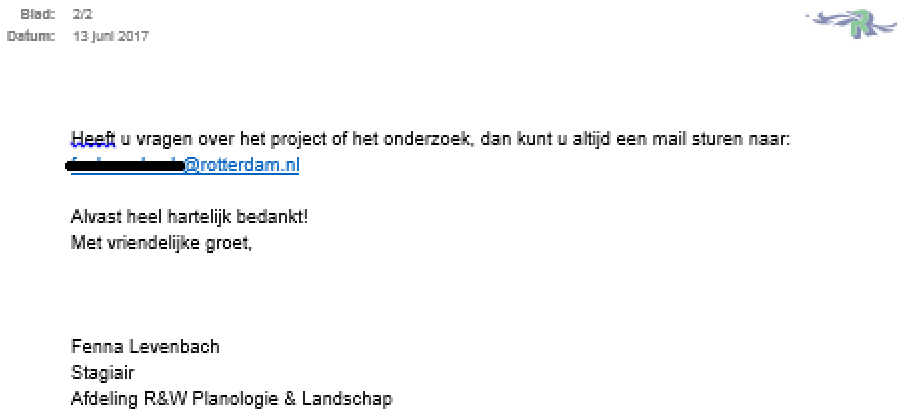
Om dat te kunnen doen is het van belang dat gegevens, zoals energieverbruik van onder andere bewoners, gebruikt kunnen worden om zuiniger en duurzamer te kunnen wonen. Daarvoor zouden bewoners bereid moeten zijn om persoonlijke gebruiksgegevens uit te wisselen, uiteraard onder voorwaarden van bescherming van de privacy.
Daarom willen we graag weten hoe bewoners denken over dit gebruik van dergelijke gegevens.

Met deze brief wil ik u vragen om mijn enquête in te vullen. Dit duurt ongeveer 10 minuten. Uw bijdrage zou de Gemeente Rotterdam enorm helpen bij het inzicht krijgen in de mening van bewoners van Hart van Zuid over het delen van persoonlijke data. Met behulp van de resultaten kan de Gemeente inzicht krijgen in hoe u als bewoner zou willen deelnemen aan een Smart City. Tevens helpt u mij met het afronden van mijn scriptie.

Link naar het onderzoek: www.goo.gl/joKF9z

De enquête is eenvoudig in te vullen via een desktop computer, maar is ook beschikbaar voor mobiele telefoons en andere apparaten.

Onder de respondenten van Hart van Zuid zullen twee VVV-bonnen van €20,- verloot worden. U kan deelnemen door uw e-mailadres in te vullen aan het eind van de enquête.



Blad: 2/2
Datum: 13 juni 2017

Heeft u vragen over het project of het onderzoek, dan kunt u altijd een mail sturen naar:
[redacted]@rotterdam.nl

Alvast heel hartelijk bedankt!
Met vriendelijke groet,

Fenna Levenbach
Stagiair
Afdeling R&W Planologie & Landschap

Figure 12: Letter to residents Hart van Zuid

Appendix B

Questionnaire - Hart van Zuid - Without Conjoint Module

Q44 Beste bewoner van Hart van Zuid,Alvast bedankt voor het invullen van deze enquête! De resultaten van het onderzoek zullen worden gebruikt voor mijn afstudeeronderzoek en intern bij de Gemeente Rotterdam. Alle antwoorden worden anoniem verwerkt.Mocht u vragen hebben naar aanleiding van deze vragenlijst of naar aanleiding van het afstudeeronderzoek, dan kunt u mij bereiken door een e-mail te sturen naar: fm.levenbach@rotterdam.nlMet vriendelijke groet,Fenna Levenbach

Q60 De gemeente wil van Rotterdam een 'Smart city' maken. In een Smart City – ofwel slimme stad – wordt met moderne technieken geprobeerd de stad te verbeteren en prettiger te maken voor de bewoners. Een voorbeeld hiervan is het Ruggedised project in Hart van Zuid. Dit is een Smart City project wat als doel heeft om energie uit te kunnen wisselen tussen gebouwen. Bijvoorbeeld door de overgebleven energie te transporteren naar omliggende gebouwen, als Ahoy leeg loopt na een evenement. Om dit te kunnen doen is het van belang dat gegevens, zoals energieverbruik van onder andere bewoners, gebruikt kunnen worden om zuiniger en duurzamer te kunnen wonen. Daarvoor zouden bewoners bereid moeten zijn om persoonlijke gebruiksgegevens uit te wisselen, uiteraard onder wettelijke voorwaarden van bescherming van de privacy. Wilt u meer weten over Ruggedised, het smart city project in Hart van Zuid, klik dan hier . Wilt u meer weten over smart cities, bekijk dan onderstaand korte filmpje met een uitleg over de slimme stad in Rotterdam:

Q50 De volgende vragen gaan over de energiemeter in uw huis. Ik wil u vragen de volgende beschreven situatie als realiteit te beschouwen: De gemeente en uw energieleverancier hebben besloten om alle energiemeters in Hart van Zuid te vervangen voor 'slimme' energiemeters. Een slimme meter is een digitale energiemeter die in de plaats komt van uw huidige elektriciteitsmeter en gasmeter. Deze meter geeft automatisch uw energieverbruik door aan de netbeheerder. De data die de meter verzamelt kan doorgestuurd worden naar de Smart City en voor meerdere doeleinden gebruikt worden.

Q52 U krijgt straks 8 achtereenvolgende keuzes te zien: De eigenschappen van de energiemeters zullen per vraag willekeurig ingedeeld zijn. Hierna wordt u gevraagd of u voorkeur heeft voor Energiemeter 1 of Energiemeter 2, afhankelijk van de gegeven eigenschappen. De verantwoordelijkheid voor het veilig opslaan van de data ligt bij.. - Hiermee wordt bedoeld wie verantwoordelijk is voor het veilig opslaan van de data. In ruil voor het delen van mijn data..– Hiermee wordt bedoeld het voordeel wat u als gebruiker van een slimme meter krijgt in ruil voor het delen van uw data met de Smart City. De data wordt gedeeld met.. - Hiermee wordt bedoeld met welke partijen uw energieverbruik data gedeeld mag worden in de Smart city De data wordt bijgehouden elk(e).. - Hiermee wordt bedoeld hoe precies de data is: Of het energieverbruik over 10 seconde , per uur of per dag wordt opgeslagen.

Q52 Waarom zou u uw data over uw energieverbruik wel of niet willen delen?

Q53 Voor welke doeleinden zou de anonieme data over uw energieverbruik gebruikt mogen worden in een smart-city? Anonieme data is niet terug te leiden tot u persoonlijk. (Er zijn meerdere antwoorden mogelijk) Om veiligheid in de wijk te bevorderen. Om de woonomgeving groener en duurzamer te maken. Om inzicht te krijgen in uw energieverbruik ten opzichte van het gemiddelde verbruik in Hart van Zuid. Niet Anders

Q47 Voor welke doeleinden zou de persoonlijke data over uw energieverbruik gebruikt mogen worden? (Er zijn meerdere antwoorden mogelijk) Om veiligheid in de wijk te bevorderen. Om de woonomgeving groener en duurzamer te maken. Om inzicht te krijgen in uw energieverbruik ten opzichte van andere bewoners van Hart van Zuid. Niet Anders

Q54 Met wie bent u bereid de anonieme data over uw energieverbruik te delen? (Er zijn meerdere antwoorden mogelijk) Politie Brandweer De gemeente Stichting Onszuidpleingebied Inwoners van Hart van zuid Studenten Start-ups Commerciële bedrijven Niemand Anders

Q48 Met wie bent u bereid de persoonlijke data over uw energieverbruik te delen? (Er zijn meerdere antwoorden mogelijk) Politie Brandweer De gemeente Stichting Onszuidpleingebied Inwoners van Hart van zuid Studenten Start-ups Commerciële bedrijven Niemand Anders

Q59 Er volgen nu drie stellingen over privacy. Hoe sterk bent u het hier mee eens of oneens? Sterk mee oneens Beetje mee oneens Niet eens of oneens Beetje mee eens Sterk mee eens Consumenten hebben alle controle verloren over hoe persoonlijke informatie wordt verzameld en gebruikt door bedrijven. De meeste bedrijven gaan zorgvuldig en vertrouwelijk om met de persoonlijke informatie die ze verzamelen. Bestaande wetten en organisatorische praktijken bieden tegenwoordig een redelijk niveau van bescherming voor privacy van de consument.

Q51 Als laatste wil ik u nog enkele algemene vragen stellen voor onderzoeksdoeleinden.

Q45 Wat is uw geslacht? Man Vrouw

Q46 Wat is uw leeftijd? 18-24 25-34 35-44 45-54 55-64 65+

Q47 Wat is uw nationaliteit? Nederlands Anders, namelijk:

Q45 Wat doet u in het dagelijks leven? Student Werk (part time) Werk (full time) Werkloos Met pensioen

Q48 Wat is uw hoogste voltooide opleiding? Geen opleiding Middelbare school MBO/ Lager beroepsonderwijs HBO/ Hoger beroepsonderwijs WO Bachelor WO Master PhD

Q54 Wat is uw burgerlijke staat? Alleenstaand Getrouwd Gescheiden/ Weduwe / Weduwenaar Samenwonend met partner Inwonend bij ouders Anders Weet niet/ Wil niet zeggen

Q55 Uit hoeveel personen bestaat uw huishouden? Volwassenen Kinderen

Q50 Heeft u een slimme energiemeter in huis?Een slimme meter is een digitale energiemeter die in de plaats komt van uw huidige elektriciteitsmeter en gasmeter. Deze meter geeft automatisch uw energieverbruik door aan de netbeheerder. Ja Nee Weet niet

Q51 Maakt u gebruik van duurzame energie? Ja Nee Weet niet

Q42 Zijn uw energiekosten inbegrepen bij uw huurprijs? Ja, de energiekosten zijn inclusief Nee, de energiekosten zijn exclusief Ik heb een koopwoning

Q53 Wanneer u op volgende klikt, wordt de enquête opgeslagen. Als u mee wil loten voor de VVV-bonnen ter waarde van €20,- vul dan hier uw e-mail adres in. Deze wordt alleen voor de verloting gebruikt.

Appendix C

Results independent sample T-test

x = 84 Students and y = 41 Non-students

```
> t.test(studentComp, nstudentComp)

Welch Two Sample t-test

data: studentComp and nstudentComp t = -1.866, df = 88.684, p-value = 0.06535
alternative hypothesis: true difference in means is not equal to 0 95 percent
confidence interval: -0.107258157 0.003370277 sample estimates: mean of x
0.2055233 mean of y 0.2574673
```

```
> t.test(studentSha, nstudentSha)

Welch Two Sample t-test

data: studentSha and nstudentSha t = 0.49064, df = 91.378, p-value = 0.6249
alternative hypothesis: true difference in means is not equal to 0 95 percent
confidence interval: -0.05141197 0.08514306 sample estimates: mean of x mean
of y 0.3216455 0.3047799
```

```
> t.test(studentSpe, nstudentSpe)

Welch Two Sample t-test

data: studentSpe and nstudentSpe t = -0.11209, df = 90.954, p-value = 0.911
alternative hypothesis: true difference in means is not equal to 0 95 percent
confidence interval: -0.06129411 0.05474598 sample estimates: mean of x mean
of y 0.2171198 0.2203939
```

```
> t.test(studentSto, nstudentSto)

Welch Two Sample t-test

data: studentSto and nstudentSto t = 1.3148, df = 113.52, p-value = 0.1912 alternative
hypothesis: true difference in means is not equal to 0 95 percent confidence
interval: -0.01943568 0.09614060 sample estimates: mean of x mean of y
0.2557114 0.2173590
```

x = In possession of a smart meter (43 respondents), y = Not in possession of a smart meter (39 respondents)

> t.test(meter1, meter5)

Welch Two Sample t-test

data: compensation t = -0.26899, df = 88.183, p-value = 0.7886 alternative hypothesis: true difference in means is not equal to 0 95 percent confidence interval: -0.07047031 0.05366705 sample estimates: mean of x mean of y 0.2190162 0.2274179

> t.test(meter2, meter6)

Welch Two Sample t-test

data: sharing t = 0.92997, df = 97.945, p-value = 0.3547 alternative hypothesis: true difference in means is not equal to 0 95 percent confidence interval: -0.04122282 0.11393087 sample estimates: mean of x mean of y 0.3334398 0.2970858

> t.test(meter3, meter7)

Welch Two Sample t-test

data: specificity t = -0.30275, df = 97.931, p-value = 0.7627 alternative hypothesis: true difference in means is not equal to 0 95 percent confidence interval: -0.07589837 0.05580581 sample estimates: mean of x mean of y 0.2177963 0.2278426

> t.test(meter4, meter8)

Welch Two Sample t-test

data: storing t = -0.54683, df = 93.282, p-value = 0.5858 alternative hypothesis: true difference in means is not equal to 0 95 percent confidence interval: -0.08292875 0.04711652 sample estimates: mean of x mean of y 0.2297477 0.2476538