GIMA
Geographical Information Management and Applications

Thesis Final Report

A smart campus as a test case for the users' perception of location data in smart cities

Thomas Molenaar

June 4th, 2020

Thesis Final Report

Thomas Molenaar

UU student number: 6192424

t.b.molenaar@students.uu.nl

Supervisor: Mr. dr. H.D. Ploeger

Professor: Dr. ir. B. van Loenen

Abstract

Smart cities are the new discourse of urban design. Almost every city strives to become smart to increase efficiency and sustainability. The concept of a smart city is actually a fuzzy concept that consists of various methods and technologies. Nowadays, many smart city technologies are in development. Herewith, privacy concerns grow. Often, citizens are not aware of the fact that they share data within these cities, they do not know what data they share and where this data is processed. Therefore, it is important to do research on the effects of technology within cities on the ground level. This type of research should focus on the effects on users and the users' ability to protect their data. To examine this, a smart campus is used as a test case in order to find out what the perspective of students is on the use of geographical data on campus. These students are questioned about their use of smart campus tools, privacy awareness, privacy concerns and their overall perception of the smart campus. These perceptions of the students are aligned with the actual situation of the use of geographical data on the campus of TU Delft. This research aims to address the difference between the assumptions of the top-down initiatives such as a smart campus and the bottom-up user perception of such initiatives. The outcomes of these differences are used and critically examined the common concept of a smart city. The results indicate a discrepancy between the perspective of students on the use of geographical data on campus and the actual use by the university. Students are not aware of what personal data is collected and for what purpose. Furthermore, the results show that a smart campus is difficult to compare to a smart city. However, the examination of it gives recommendations and directives for the design and implementation of technology in cities. Hereby, technology should mainly be used for specific purposes that contribute to participation and democratization. Smart cities that are developed from a commercial point of view are likely to create a city wherein citizens are constantly monitored and wherein life for the citizen is as user-friendly as possible. In the long term, this may lead to social and economic inequality and unattractive cities.

Preface

This thesis in front of you has been written as part of the Master Programme Geographical Information Management and Applications of the University of Utrecht, Technical University of Delft, Wageningen University and the University of Twente.

The subject of a smart city from a user's perspective is not very common within the GIMA subjects. However, every person that works with geographical data is affected by it. In fact, every person in society is affected by the way we use geographical data. Working on such a relevant and complex problem was really challenging and eye-opening. In the end, I am glad that I broaden both my scientific knowledge about geographical data in our lives as well as my consciousness about what opportunities we have in our digital age.

The research for this thesis took place from September 2019 till June 2020. A substantial part of the research is conducted during the COVID-19 crisis, which was a memorable experience. The developments in this crisis certainly interweave with the question how data should be used and applied in our society.

I would like to thank Hendrik Ploeger as supervisor and Bastiaan van Loenen as responsible professor for their time, input, interesting perspectives and their constructive feedback. Furthermore, I would like to thank all the 153 students from TU Delft that participated in the survey and that reacted very positively and openly to the research. Lastly, I would thank all the people that made so much effort to keep me on track.

Enjoy your read.

Tom Molenaar,

Amsterdam, June 4th, 2020

Table of contents

1. Introduction

1.1. Context

In 2017, the company Sidewalk Labs was selected by the governmental organization Waterfront Toronto as innovation and funding partner for the Sidewalk Toronto project (Sidewalk Labs, 2019). This gave Sidewalk labs the exclusive right to work with Waterfront Toronto and other governmental partners to plan and develop a new district in Toronto's Eastern Waterfront. Sidewalk Labs, which is a company of Google's holding company Alphabet, promised that it will build a city 'from the internet up' creating 'the first truly 21st-century city' (BBC News, 2018). They aim to create the 21st-century city by a redevelopment plan that combines the physical layer of the city with a digital layer on it (Sidewalk Labs, 2019). Smart-city technologies will be infused in urban morphology (Peel & Tretter, 2019). This means that both the hardware and the software in the area will be in the hands of the technology company (CityLab, 2019).

However, a few months after the official announcement of Sidewalk Toronto, questions about the motivation of the involvement of Alphabet began to arise (Peel & Tretter, 2019). According to Peel & Tretter (2019), critics stated that it was not clear which rights the holding company of Google would have regarding the use and the processing of data. There are still no specific plans about data ownership or control which stoke up concerns about data even more. Peel & Tretter (2019) state that Sidewalks' attempt led to a reputation of a 'new-urban pirate' amongst critics.

This particular development shows that on the one hand, the futuristic idea of a smart city is almost here and fast approaches, but that on the other hand it raises a lot of questions. The smart city is an often-described concept in both scientific literature and media. It should be the solution for most of our contemporary and future urban challenges (AMS Institute, n.d.). Examples of these challenges are smart mobility, energy, climate-resilient cities, metropolitan food systems, responsible urban digitization, and circularity in urban regions (AMS Institute, n.d.). After all, it is about the implementation of ICT and data in the urban environment (Dalla Corte et al., 2017).

The smart city seems a very optimistic and realistic prospect. However, little attention is paid to the consequences for the citizens and the urban life. Batty et al. (2012) state that smart cities consist of data that is collected through sensing hand-held and remote devices which measures how individuals and groups use information, interact and move. It is unknown what will be the impact on society. All these developments may have advantages but will undoubtedly also have disadvantages regarding questions of privacy and confidentiality (Batty, 2013). These questions of privacy and confidentiality mostly will have an effect on the citizens, since they are big collectors of data via crowdsourcing.

In the book "Open Data Exposed", Van Loenen & Ploeger (2018) outline two scenarios for the smart city in 2050. In one scenario, they describe life in the smart city as a life that is dominated by decisions that are made based on data and algorithms designed to a citizens' personal situation. Both the data and the algorithms are not controlled by the citizen and access is not possible. The data and algorithms are owned by a limited number of organisations that are dependent on another.

Van Loenen & Ploeger (2018) argue that the result is a “de facto data dictatorship” which is developed by a group of worldwide enterprises. In similar literature, this is also named a surveillance state that uses smart technologies to monitor its citizens (Galdon-Clavell, 2013). Zuboff (2019) presents the term surveillance capitalism. In surveillance capitalism, human actions are recorded and transformed into data, which is the raw material for predictive products by machine intelligence.

In the other scenario for 2050 from “Open Data Exposed”, the world is completely different from the ‘darkening of the digital dream’ as described by Zuboff (2019). In the other scenario, the citizen itself is fully in control about what is shared, when, with whom and for how long (Van Loenen & Ploeger, 2018). The citizen is empowered and aware of privacy. Data is by default open and there is a certain sense of data democracy. A similar concept is the coordinative smart city, as envisaged by Richard Sennet, which will be discussed in the theoretical framework.

1.2. Problem statement

This introduction leads to the problem that is addressed in this research; Municipalities and cities are willing to become smart and give up their control to companies (Naafs & Ettema, 2017). The label smart is considered as the method to be prepared for the future. If cities and municipalities become smart, there will be a huge increase in the amount of collected and processed data within the city. This information is especially from and about the citizens, such as in the Toronto example. Moreover, there are often tech companies involved, from the ‘big five tech giants’ (Facebook, Amazon, Apple, Microsoft and Google), in the development of becoming smart. With these developments in mind, questions arise about who should be the owner of the data and should that data be collected at all? Do citizens know that they are being tracked within a smart city and that they share data via all kinds of sensors? Or do people accept the fact that they share data and that this is the way to make their life easier? To put it briefly, how do people perceive privacy of their personal data within smart cities?

The all-embracing perception of the smart city from a commercial and business perspective is often described, while there is little attention for debate about data ownership and privacy of citizens within the city (Van Zoonen, 2016). Is the scenario, in which we will face a surveillance state, imaginable? A state where every step we take is recorded? Or are we already in it and if so, how far?

This thesis will elaborate on the privacy perception of citizens within the smart city that concerns data, with a specific focus on geographical data. Geographical data that people share with the rest of the world through their handheld devices. Surely, perception is an intangible concept. However, the concept will, of course, be explained further in this thesis in the theoretical framework and within the operationalization. Nevertheless, to shortly clarify it, in this thesis the perception of privacy is similar to the perception of safety, in which there is an objective dimension and a subjective dimension (Austin, Furr & Spine, 2002). These dimensions may be unbalanced or unequal (Dinev & Hart, 2004).

1.3. Research question

These questions of the problem statement are more concisely formulated into one main research question and 6 objectives. The main research question in this thesis is the following:

"What can be learnt from the students' perception of location data on campus in comparison to the actual state at TU Delft, for the design of future smart campuses and smart cities?"

This study aims to answer this question through a study about current use of geographical data on campuses and experiences with geographical data on campus, by a population of students at Delft University of Technology in the Netherlands. Hereby, perception is considered as the way someone thinks and feels about geographical data. The outcomes should contribute to the debate about the organisation of technology and data within society. This research focuses thus specifically on the field of smart cities and smart campuses. The outcomes of the study should give new understanding in the design for a user-empowered smart city and smart campus, which means that the users are aware and in control of the data they share.

To do research to all those questions and concepts might be a bit ambitious and challenging. The topics are very broad and the subjects are multidisciplinary. For that reason, it was that the scope of the research and the framework is scaled down to a smaller and less complicated test case of a smart campus. Nowadays, many campuses all over the world experiment with artificial intelligence and big data to improve learning and living on the campus (Niemtus, 2019). Hence, the movement towards a system with the label 'smart' also applies to universities. The difference between a smart city and a smart campus is that smart campuses are probably easier to implement since there are fewer players and stakeholders involved, according to Niemtus (2019). Besides that, the university is often the owner and manager of the real estate and networks. This also applies to the campus of TU Delft, where the university is the owner and manager of all the real estate and where the university is responsible for all campus developments (TU Delft, n.d.). Many smart city technologies are tested on smart campuses and Bates & Friday (2017) state that a campus reflects in many ways a city in miniature.

To answer the research question, both a secondary analysis will be performed and a survey will be conducted among students on campus at TU Delft. First, the current tools and techniques for the implementation of smartness at international campuses, Dutch campuses and the campus of Delft are to be investigated, based on secondary sources. Thereafter, these findings are incorporated in the survey and presented to the survey respondents. The survey is extensive and divided in two parts. While filling in the survey, the students are informed about the various tools and techniques that are already in use on campus at TU Delft or on other campuses. Based on this information transmission there is tested if this new information changed the perception of the respondents. Besides the current smart campus tools, hypothetical tools or tools that are pilots on other education institutes will be introduced to examine if the respondents are likely to use the tools. In the end, the outcomes can be useful to research the perception of the students regarding their data and thereafter for the design of a user-empowered smart campus. The findings will be linked and generalized as much as possible to the smart city concept and design, as described in the theoretical framework.

Considering the study from the respondents, the outcomes of the survey will also be used to answer the question if students, that belong to a particular faculty, have higher or lower awareness and experience higher or lower concerns of location data that they share. In short, if they have a different perception of location data.

1.4. Research objectives

The research objectives are the specific research actions that are carried out in this study. The objectives embody the structure of the whole thesis and are used to support the process of answering the comprehensive main research question. The objectives are formulated as the following:

I. Explore how geographical data from students is used on international campuses, Dutch campuses and on the campus of TU Delft in particular.

II. Understand what the perception of students is on campus at TU Delft, regarding the geographical data that is collected about them.

III. Analyse which smart campus tools that collect and process geographical data from students are used at the campus of TU Delft.

IV. Evaluate if the perception changes when students are informed of the geographical data processed by smart campus tools and if there is a discrepancy between the actual state of the smart campus and the perception.

V. Make recommendations for the design of a user-empowered smart campus and smart city policy.

To achieve the objectives, a variety of methods is used. Objective I and partly objective III are completed through a secondary analysis. Different articles and books are hereby consulted and discussed. Objective II and IV are completed through a conduction of a survey. Objective IV is the basis for the recommendations of objective V. The design of objective V is also based on processed literature in this study about the design for smart campuses and smart cities.

1.5. Scope

The main focus of this thesis is the perception of the usage of geographical data from students on the Campus of the TU Delft. Whereby TU Delft is the research area. This means that people will be questioned about their behaviour and experiences with the processing of their data on the Campus' territory. The behaviour and experiences of data processing are mostly focused on location data, but other personal data is also researched. In addition, the actual state of smart campuses on an international scale is also researched through secondary sources, as well as other Dutch campuses. In this research, the definition of the usage of data is all the data that a student shares with its device or data that is tracked from them by sensors.

The approach is to find out what students think that happens with their geographical data and to reflect that to what is actually happening on campuses. It focuses thus on the discrepancy between the perception of the users and the real situation, as described in the problem statement with the perception of safety.

For the researched data, this means that the research is specifically focused on shared data, either passively or actively, from students on campus. The students that make up the population for the survey are solely students from TU Delft. Hence, support staff and researchers are out of scope. Furthermore, the aim is to create input for the design of future campuses and cities that strive to become smart. This input for the design will describe how students on smart campuses should be involved in the development and what the role the data should play. In the end, the outcomes of the research will be linked to the narrative of smart cities to find similarities and to draw conclusions on a broader perspective.

In this study, the campus is defined as: “all the land and buildings that are in use by university functions or functions related to the campus, whether leased or owned by the university, and not bound to a single location” (Valks, Arkesteijn & Den Heijer, 2018, p.21).

The timespan in this research is from September 2019 to May 2020, which means the research was already in an advanced stage when the COVID-19 crisis began. Therefore, the effects of the crisis are out of scope in the research.

1.6. Relevance

As stated earlier, the subject of this thesis is highly relevant from both a scientific perspective and a societal perspective. It is scientifically relevant because research about politics of data in a smart environment is relatively scarce (Van Zoonen, 2016). In literature, little attention is paid to the control and privacy of users. Moreover, many scientific articles and books describe smart cities and smart campuses from a technological perspective while they do not focus on the effects on citizens and society in the long term. This particular approach is what this study adds to the current body of knowledge.

Of course, the subject has a high societal relevance as well, as already is demonstrated in the introduction. The smart city concept aims to make cities more efficient and more sustainable, which are very popular and important subjects in daily news and debates. In addition, this thesis concerns the themes of digitalization and privacy. There is a growing and ongoing movement about the perspective on our digital future. Many writers, such as Soshana Zuboff and Yuval Noah Harari warn of the impact of technology in our society. Yuval Noah Harari describes that artificial intelligence will generate huge changes to society in the 21st century (Harari, 2018). An example is change in equality, which is also endorsed by Zuboff. They both state that those who own the data own the future (Harari, 2018; Zuboff,2019). Harari calls upon lawyers, politicians, philosophers and even poets to focus on this question.
Moreover, digitization has a huge impact on the lives of citizens and it increases the risk of loss of privacy (Ståhlbröst, Padyab & Hollosi, 2015). The outcomes of this research can contribute to the design of a citizen-empowered and a user-empowered smart campus or smart city. That makes research in these subjects relevant.

1.7. Reading guide

This thesis is structured in 6 different chapters. After this first chapter, the second chapter provides an extensive literature review to identify the three themes: the smart city, the smart campus and privacy. Chapter 3 will specify the approach of the research and the methods that are used to carry out the research. Then, chapter 4 first presents the results of the secondary analysis, followed by the results of the quantitative analysis of the survey. Afterwards, in chapter 5 and 6, the conclusions are drawn. Finally, in chapter 7, the discussion, recommendations for design and recommendations for further research are discussed.

2. Theoretical framework

Within this theoretical framework, theories that relate to the research question are defined and discussed. The context of already existing literature, wherein this thesis is embedded, is outlined. At first, the general perspective of the smart city and the smart campus will be defined. Thereby, the way a smart city and a smart campus are spatially enabled in terms of geographical data is described. After that, criticism of and perspectives on smart cities are discussed. This criticism focuses on how the smart city functions and what the impact may be on the citizens. The last part of the theoretical framework focuses on privacy. The comprehensive concept of privacy will be described with all its aspects that are relevant to this study. The theory of privacy will be discussed convergently, which means that it starts with more general theory about privacy and then it directs towards more case-specific theory of location privacy and perception of privacy.

2.1. Smart city, Smart campus and geographical data.

2.1.1. Smart city

When the concept of the smart city is analysed, it turns out that the concept of the smart city is actually a fuzzy concept (Dalla Corte et al., 2017). At different places around the world, local governments encourage technological and economic developments that all come together under the popular policy label of ‘smart cities’ (Caragliu, Bo, & Nijkamp, 2011; van Zoonen, 2016). Smart city is an umbrella term, which consists of different technological instruments at various scales that provide networks of continuous data about people and materials in the city (Batty et al., 2012). However, according to Batty et al. (2012), cities are only smart when these technological instruments are integrated into intelligent functions and synthesized in a system. Furthermore, these technological instruments should serve a specific purpose. In an in-depth literature review, Albino, Berardi, & Dangelico (2015) aim to clarify the meaning of a smart city. They ended up with the four most common characteristics of smart cities. These characteristics are:

- A city’s networked infrastructure that enables political efficiency, social development and cultural development
- An emphasis on business-led urban development and activities for promoting urban growth
- Inclusion of residents and social capital in urban development
- The natural environment as a strategic component for the future

Martínez-ballesté, Pérez-martínez, & Solanas, (2013) state that most of the services that are offered within a smart city are based on ICT. Sensors and wireless networks have become the basis of the smart city (Roche, 2014). The user of the smart city uses a device, such as a smartphone, that interacts with these services. The active engagement of the citizens is a major requirement to make cities smarter (Roche and Rajabifard, 2012). The smart city refers to the use of ICT within the urban environment, which indicates the digitalization of cities (Dalla Corte et al., 2017). In addition, domains from ICT and engineering use the smart city concept to advocate the fact that information and communication technologies improve urban infrastructures and its efficiency (Roche, 2014).

2.1.2. Geographical information and the smart city

Within a smart city, there is a key role for location data or geographical data (Roche, 2014). As stated earlier in the definition of the smart city, active engagement of citizens plays a significant role in the smart city. This role requires citizens to be spatially and digitally enabled in the smart city (Roche and Rajabifard, 2012). Roche & Rajabifard (2012) state that a smart city needs a platform that aggregates data from citizen sensors and device sensors. “The smart city is not a machine, but it is made by local actions and feelings from people, with a spatial data infrastructure (SDI) at the heart of the smart city” (Roche and Rajabifard, 2012).

In this thesis, the definition of geographical information and its characteristics are the following: geographical information is spatial data that is related to a location on the surface of the earth (Huisman & De By, 2009). According to Huisman & De By (2009), geographical data strictly is data that is derived from spatial data. However, they state that in day-to-day use, it is allowed to exchange spatial data and geographical data.

2.1.3. Bold Cities

Nowadays, cities thrive on all kinds of data that tend to help local governments and businesses to monitor, plan and innovate (Centre for BOLD Cities, n.d.). However, it is unclear how the people, of which every feature, behaviour and movement is monitored, benefit from the Big, Open and Linked Data cities (BOLD cities).

BOLD cities use all kinds of data that is generated by sensors, social media and classic census data. These data consist of real-time data, historical data, impersonal data, personal data and individual data. This raises questions about storage, analytics, visualization and presentation. Besides that, it also raises questions about appropriate data-governance and management. This governance and management should mainly be focused on the social and individual consequences of the urban data revolution for people in the city.

2.1.4. Smart campus

In contrast to the concept smart city, a smart campus is a less common term in scientific literature and popular media (Vasileva et al., 2018). However, there is literature that addresses the smart campus, albeit fragmentally or specified to one particular technology. Vasileva et al. (2018) state that just as with smart cities, the private sector tries to conceptualize the smart campus in order to offer smart solutions.

Agate, Concone & Ferraro (2018) also make the comparison between the smart campus and the smart city. They state that a campus represents a cross-section of the urban fabric on a small scale. Furthermore, they argue that it is possible to improve services that are provided to the students, staff and teachers through information that is collected and shared by heterogeneous sensors. Overall, literature of smart campuses is mostly about digital technology without connecting it to wider aspects of an academic institution (Vasileva et al. 2018)

2.1.5. Geographical information and the smart campus

As stated in the definition of the smart campus, the literature about the smart campus is much more fragmented. This means that the link between geographical information and the smart campus is also less described. Therefore, the link between geographical information and the smart campus is also researched within this thesis.

When the smart campus is described it frequently concerns technical tools for the smart campus. Therefore, technical and smart tools will be summarized in this section to explain the link between geographical information and the smart campus. The variety of data on a smart campus is less comprehensive, as can be read below, than in a smart city.

Valks, Arkesteijn & Den Heijer (2018) compare six different tools that are used at international universities, which they define as smart tools. These tools are used to find available study places, to optimize teaching space use, to share teaching space for studying, to find shared workspace, to align building use and energy use and to improve meeting room use. Measurement methods are via access gates, infrared sensors, Wi-Fi, PC login data, workplace check-ins and videoconferencing system reservations. Thereby, most of the data of the tools is presented real-time. The tools will be further discussed and explained in the results of the secondary analysis (Section 4.1).

2.2. The other side of the smart city

In this section, critical literature on the concept of smart city, as described up to now, is discussed.

2.2.1. The prescriptive smart city versus the coordinative smart city

Tyler Durden: “Stop being perfect, because obsessing over being perfect stops you from growing.” (Fight Club, 1999).

Similar to the scenarios of the data-dictatorship and the data democracy, Richard Sennett introduces a typology of smart cities. He distinguishes two different types of smart cities in “Building and Dwelling: Ethics for the city”, to wit, the prescriptive city and the coordinative city (Sennett, 2018). In this section, the prescriptive smart city and the coordinative smart city will be explained and discussed.

In the prescriptive city, whereby the data-dictatorship scenario comes to mind, the city is filled with user-friendly technologies. Sennett describes that these user-friendly technologies insult the intelligence of the citizens because they make the city too easy to live in. He states that these urban technologies tend to make cities cleaner, safer and more efficient. Such a smart city is thoroughly driven by politics of centralized control.

Sennett questions what the perspective of the prescriptive smart city is on the ground level. For this perspective on the ground level, he mentions two examples of existing cities: Songdo in South-Korea and Masdar City in the United Arab Emirates.

In his book, practices and techniques in these cities are extensively narrated. Both cities are created from scratch with technology woven into the fabric of the cities. In the city of Songdo, the control is centred in, as Sennett calls it, a cockpit where all data is monitored and where algorithms try to achieve optimal efficiency in controlling the city. Based on big data, the city is operated and orchestrated.

Such a cockpit metaphorically symbolizes the prescriptive smart city. Songdo is designed to improve its international competitiveness, in terms of lower commercial taxes and fewer regulations for trade.

Masdar City, in Abu Dhabi, is an example that is designed to reduce the ecological footprint. Hereby, advanced sustainable technologies are used and combined in a powerful computer that takes care of the big data, on which the governance of the city is based. Sennett describes that during his and his researchers' visits to Songdo, their impression of the city shifted from a dream of a planned city with ubiquitous computing to a heavily monitored city without much diversity or democracy.

According to Sennett, the goal of the technologies in the smart city of Songdo is to make the life of the users as user-friendly as possible. He states that this leads to ''stupefied" users that do not think for themselves. His researchers also found that smart cities are so easy to live in. Furthermore, another characteristic of the prescriptive smart city is the limitation of chance, in which there is no place for serendipity. Within a prescriptive smart city, a too-tight fit between form and function results in a predictable place without friction.

In addition to the criticism of Sennet, Hajer (1999) presumes that a new brief of urban design is aimed at avoiding the unknown. This new brief is part of a broader shift in the way the urban realm is perceived. Within the urban realm, controllability is what matters. He states that we very carefully pick the spaces in which we want to be. This leads to a zero-friction society in which people are on the move without sacrificing any communicative connectivity. According to Hajer, these places are not truly urban. Furthermore, designers work with briefs which are dominated by missions as avoidance of congestion and crowd management. The importance for development of places for meaningful human interaction decreases. Nevertheless, Hajer points out that he does not declare that places as terminals and shopping malls do not function. However, people's behaviour at such places is heavily monitored and governed through disciplinary systems. Therefore, these places should be seen as well-disciplined monocultural zero-friction enclaves. To resist this, Hajer argues that the development of the public domain as a realm where ideas are exchanged, political arguments take place, opinions change and preferences are formed, might be a new brief for urban design.

Somewhat similar applies to the prescriptive smart city as described by Sennett. Even though the monocultural zero-friction enclaves arise from transport and the prescriptive smart city emerges from technologies to become smart, both the prescriptive smart city of Sennett as the mono-cultural zero-friction enclaves of Hajer arise from the desire to control and predict.

Sennett indicates that the prescriptive model deadens curiosity. The possibility that leads to a dead-end will not be pursued because this will disrupt the balance within such a system. As in navigation programs such as TomTom or Google Maps, people are prescribed how to get from point A to point B along the most efficient route. The consequence is that people move through space without experiencing place. Ultimately, by reducing people's lives to digital bits and using machines, people would stop learning and would become stupefied in the prescriptive smart city (Sennett, 2018).

In contradiction to the prescriptive smart city, Sennett considers the coordinative smart city as a solution for the stupefaction. Within this coordinative smart city, technology is used to coordinate instead of control, which results in a completely different type of smart city. He states that coordinative technology develops human intelligence because it focuses on people as they are rather than on how they should be. The fact that these technologies are cheaper is an additional benefit, according to him.

The development of these coordinative smart cities is achieved through the creation of open networks. Open networks are inclusive and people within the city have control over their feedback of data to the network. Coordinative smart cities honour limitations on their own data. Therewith, the data that is processed is shared with others. Contrarily, closed networks constantly receive feedback from citizens, whether the citizens agree with it or not. Sennett introduces Porto Alegre in Brazil as an example of such an open urban network. In Porto Alegre, economic resources are distributed bottom-up and the citizens participate in the budgeting process. Although the data was not very accurate at that time, the access to participate was open. However, when the city expanded, coherence was lost. Migrants were no longer integrated into the organizations and they were not able to take part in participatory budgeting.

Nevertheless, with the rise of big data and the smartphone, it becomes possible to coordinate participation in the smart city on a large scale. The data that comes online is not an end product and is still debatable. Online platforms operate at local levels to assemble views and responses. Elected representatives represent the feedback from these platforms. The budget is binding, and the council have the opportunity to suggest changes but is not required to do so.

Sennett argues that as in budgeting, the design of the smart city itself also can follow an open, coordinative form where citizens can control their own fortunes. In this way, it is possible for planners and citizens to ask what-if questions and to compare the responses that emerge from these questions. The technology adds huge value through immediate computation of consequences of the proposed plans. The benefit is that this shortens the time span which enables planners and citizens to change plans directly.

Hence, the major difference between the prescriptive city and the coordinative city is that high tech in the coordinative city helps people to choose instead of decisions that are made by algorithms, such as in the prescriptive city. In the coordinative city, people have far more input in data. With an open urban design, citizens are able to see alternatives and to make decisions. The prescriptive city is a hermetic system, while the coordinative city is hermeneutic. The consequence is that the coordinative city is more susceptible to mistakes. From a political viewpoint, the prescriptive city tends to be authoritarian, while the coordinative city tends to be more democratic.

Hajer (2014) argues that planning of smart cities could be successful if its configuration is able to change and to adjust constantly and continuously. Moreover, he states, it will all be about networks. According to him, urbanism in the twenty-first century should become a project of feedback on feedback that needs to be the condition for continuous learning, reflection and adjustment, which can only be done via open networks and sharing experiences and solutions.

2.2.2. Surveillance Capitalism

In addition to the metaphorical cockpit of Sennet, Shoshana Zuboff claims that there is a new economic logic that she calls “surveillance capitalism” (Zuboff, 2020). Zuboff states that: “Its success depends upon one-way-mirror operations engineered for our ignorance and wrapped in a fog of misdirection, euphemism and mendacity.” (Zuboff, 2020 p.30)

The rise of this surveillance capitalism went largely unchallenged. Digital was fast and the digital services were considered as free. But now, it seems that the surveillance capitalists, that offer those services, see the people as the free commodity. Zuboff states that people thought they search Google, while in reality, Google searches the people.

These delusions of surveillance capitalism rest on the misleading belief that privacy is private. It is imagined that the degree of privacy can be chosen with an individual calculation in which a bit of personal information is traded for valued services. In fact, privacy is not private. The effectiveness of these private and public surveillance and control systems depends upon pieces that a person gives up of itself, or that is secretly taken.

The delusion of privacy as private feeds social divide and asymmetries of knowledge and power. The surveillance capitalists exploit the widening inequity of knowledge for profits and thereby they endanger not only individual privacy, but also democracy.

Surveillance capitalism starts with a unilateral claim to private human experience as free raw material for a translation into behavioural data. These data flows are conveyed through complex chains of devices, tracking software and monitoring software. Thereafter, these flows end up in computational factories called artificial intelligence. These data flows are manufactured in behavioural predictions that are about us, but not for us. They are sold to markets that trade in human futures. This new form of trade created very rich and powerful companies. Many companies, therefore, shift their business models towards surveillance capitalism. First Facebook migrated, then the tech sector migrated and now the rest of the economy migrates, such as insurance companies, educational institutes, health care facilities and every other product that begins with the word “smart” or “personalized”.

Surveillance capitalism economics is based on the competition to sell certainty. Machine intelligence must feed volumes of data. However, the algorithms also require varieties of data. The algorithms want to know as much as possible. Unequal knowledge about people produces unequal power about people. They have become targets for remote control since surveillance capitalist found out that most predictive data come from the intervention in behaviour. Hereby, actions are modified in the direction of commercial objectives.

The surveillance capitalists have the knowledge, the machines, the science and the scientists. All privacy now rests with them. Without law and in the absence of declarations, surveillance capitalism threatens society and unmakes democracy. Surveillance capitalists are rich and powerful, but they are not invulnerable. The capitalists fear lawmakers, who do not fear them.

2.3. Privacy

The first two sections processed theory on the part of the research question and the objectives that concerned the smart city and the smart campus. The next section elaborates on the part of the research question of privacy and the privacy perception.

2.3.1. General privacy

Article 8 of the European Court of Human Rights dictates that ‘’everyone has the right to respect for his private and family life, his home and his correspondence.’’ (European Court of Human Rights, 2019). Nonetheless, many people consider privacy as a fundamental right, without being able to precisely define it (Beresford & Stajano, 2003). The term privacy is indeed difficult to define because it varies widely regarding environment and context (Banisar & Davies, 1999). However, Banisar & Davies (1999) state that it is often seen as a way of drawing a line to what extent society can intrude into a person’s affairs. Instead of seeing privacy as a right, many researchers argue that privacy is the ability of individuals to control information about themselves (Bélanger et al., 2002)

Alan Westin, who wrote the book “Privacy and freedom” about the modern understanding of privacy, defines privacy as follows: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967, p. 7) Privacy is often divided into four different categories (Banisar & Davies, 1999; Clarke, 1999):

- Information privacy, which stands for regulations governing the collection and handling of personal data. Furthermore, individuals claim that their data should not automatically be available to organizations or other individuals. Besides that, individuals should have a substantial degree of control over their data if this is possessed by others.

- Bodily privacy, which stands for the aspects of privacy that concern the protection of people’s physical beings against invasive procedures. Issues that are associated with this type of privacy are for example blood transfusion without consent, imposed treatments such as sterilization and requirements for submission to biometric measurement.

- Privacy of personal communications, which stands for covering the security and privacy of mail, email, telephones and other types of communication. This type of privacy also includes interception privacy.

- Territorial privacy or privacy of personal behaviour stands for issues that relate to sensitive matters, such as political activities, religion and sexual preferences. In fact, private space is vital to all aspects of behaviour, such as intrusion into the domestic and even public spaces.

2.3.2. Mosaic theory

Smart cities are producers and consumers of big data (Edwards, 2016). According to Edwards (2016), in both cases the big data in the smart city does not need to involve personal data. However, he states, the smart city will almost invariably do so. Through datamining across different datasets, a known person can be identified, even when these datasets are anonymized. This effect is called the mosaic effect (Edwards, 2016). Kugler & Strahilevitz (2016) state that the mosaic theory assumes that the whole is bigger than the sum of the parts. More concretely, this suggests that an entity can learn more from a given slice of information if that slice can be put in the context of a broader pattern, which is described as a mosaic (Kugler & Strahilevitz, 2016).
This means that someone's personal life can be constructed from meaningless individual pieces of information to thousands of data points combined which leads to a meaningful picture (Simmons, 2019).

What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene (Simmons, 2019 p. 119).

2.3.3. Information privacy

Nowadays, when most communications are digitized and stored as information, the privacy of communications and information privacy can be seen as one category (Bélanger & Crossler, 2011). For information privacy, the definitions also vary widely. Most definitions include some form of control over the data-usage for another purpose then it was originally collected for (Bélanger et al., 2002). Information privacy is identified in four dimensions by Smith et al. (1996). These four dimensions are: collection, unauthorized secondary use, improper access and errors. Another definition is ''the interest an individual has in controlling or at least significantly influencing, the handling of data about themselves" (Clarke, 1999). The interest grew during the 1960s and is often directly linked to the concerns about the accelerating capability of computers (Clarke, 1999). If more information about people is obtained by the use of interconnected devices, it will become harder for people to prevent information about their life from being known to others (Song, Fink & Jeschke, 2017). On top of that, technologies, effectiveness of collection, storage and analyses of immense amounts of data has definitely increased over the past years. These conditions lead to increased concerns over potential erosion of personal privacy (Norberg, Horne & Horne, 2007).

Nevertheless, individuals are open to share personal information in exchange for small rewards or perceived benefits (Kokolakis, 2017; Norberg, Horne & Horne, 2007). Pötzsch (2009) explains that even if people have a theoretical interest in the protection of their privacy and personal data on the Internet, research to their actual online communication shows an opposite behaviour. This discrepancy seems to be a paradox. The paradox where individuals express their concerns about intrusion of privacy and still are willing to give their personal information for something in return is called the privacy paradox (Kokolakis, 2017).

However, few studies show empirical evidence of this asymmetrical exchange, whereby the consumer receives limited value for the information that they provide to a firm (Norberg, Horne & Horne, 2007).

2.3.4. Privacy awareness

The behaviour in the privacy paradox is often a consequence of lacking privacy awareness (Pötzsch, 2009). Pötzsch (2009) states that privacy awareness enables people to make more informed decisions and to make fewer decisions that are privacy-invasive. The definition of awareness is as follows: "awareness is based on an individual's attention, perception and cognition of physical as well as non-physical objects. The state of being aware of something fades away as soon as there is no longer any stimulus present. Information from the environment or from other people constitutes such stimuli" (Pötzsch, 2009, p. 3).

According to Pötzsch (2009), the privacy awareness of an individual encompasses the attention, perception and cognition of four components. The first component is whether others have received or receive personal information about the individual, the presence of the individual or the activities of the individual. The second component is which personal information others receive or have received. The third component encompasses how the information is processed and used or may be processed and used. The fourth and last component encompasses the amount of information about the activities and presence of others that might reach and/or interrupt the individual.

2.3.5. Privacy concerns and the perception of privacy

In this section, theory about the perception of privacy and privacy concerns will be discussed. Dinev & Hart (2004) argue that the developments of storage technologies and digital networks increased along with concerns over protecting privacy. Dinev & Hart (2004) aimed to research the underlying antecedents of privacy concerns, which are perceived vulnerability and the perceived ability to control personal information using the Internet.

These two factors cause privacy concerns when a user decides to disclose information or not. According to Petronio (2002), vulnerability describes the perceived potential risk when personal information is disclosed and can be understood as a factor that determines the individuals' experience and the perceived state of privacy. Culnan & Armstrong (1999) state that individuals will perceive the disclosure of information less privacy-invasive when they think they will keep control of the information in the future. When the future use of the information is not known or the individuals are not able to control the information, they will resist to reveal it.

If the perception of an individual is that the information will not be used fairly and negative consequences stick to it, the individual will be less likely to engage in an Internet activity that requires disclosure of information. However, individuals that experience a positive outcome of information disclosure, for example a job offer, perceive fewer privacy invasions than individuals that experience a negative outcome of information disclosure (Dinev & Hart, 2004). Stated differently, privacy concerns are determined by the perception of the outcome of information disclosure. In addition, the perception of vulnerability can be dependent on any experience from an individual.

In the study of Ackerman et al. (1999), the focus is on the level of comfort of people's attitude to online privacy. The outcome of the study is that the concern of people depends on what type of information they should deliver and on the usefulness to the user.

In short, individuals will have fewer privacy concerns when they perceive they have control over the information. This does not equally mean that this perception is the real privacy situation. Environmental aspects and interpersonal elements may create the perception of privacy (Dinev & Hart, 2004).

2.3.6. Privacy security

In this section, the General Data Protection Regulation (GDPR) will be briefly discussed. The GDPR applies to every member state of the European Union (EU, 2016). It is focused on: "the protection of natural persons with regard to the processing of personal data on the free movement of such data" (EU, 2016 p. 1).

This GDPR safeguards the right to the protection of personal data which contains the following principles: the need of a legal basis for processing personal data, a careful design, technical and organizational measures and the right for people to be in control (Autoriteit Persoonsgegevens, n.d.). The legal basis for processing personal data are consent of the user, vital interest, legal obligations, contractual necessity, public interest and legitimate interest. A careful design consists of a data protection officer, privacy by design and an impact assessment. Technical and organizational measures include a processing registry, a data protection policy and digital security. The right for people to be in control contains the right of access, the right to rectification, the right to be forgotten, the right to data portability and the right to be informed.

2.3.7. Threats

In order to frame threats to privacy, the four quadrants of (un)authorized access/use of Choenni et al. (2016) are used. These quadrants are based on the way citizens are involved in data collection. Crowdsourcing makes it easier to involve citizens in the process of data collection. Citizens easily collect data about several phenomena with their smart devices. However, Choenni et al. (2016) state that citizens are not always actively involved when they collect data, they may also collect data passively and unknowingly. The users may not be aware which data an application collects and to which organisations this is passed. Besides that, users do not change or do not know how to change the default tracking settings.

The first categorization of the quadrants is the criterion whether access to data is authorized or unauthorized. The second categorization is the criterion if the data usage is authorized or unauthorized. These criteria are directly linked to data privacy and data misuse. These quadrants are described in a scheme with various examples, see figure 1.

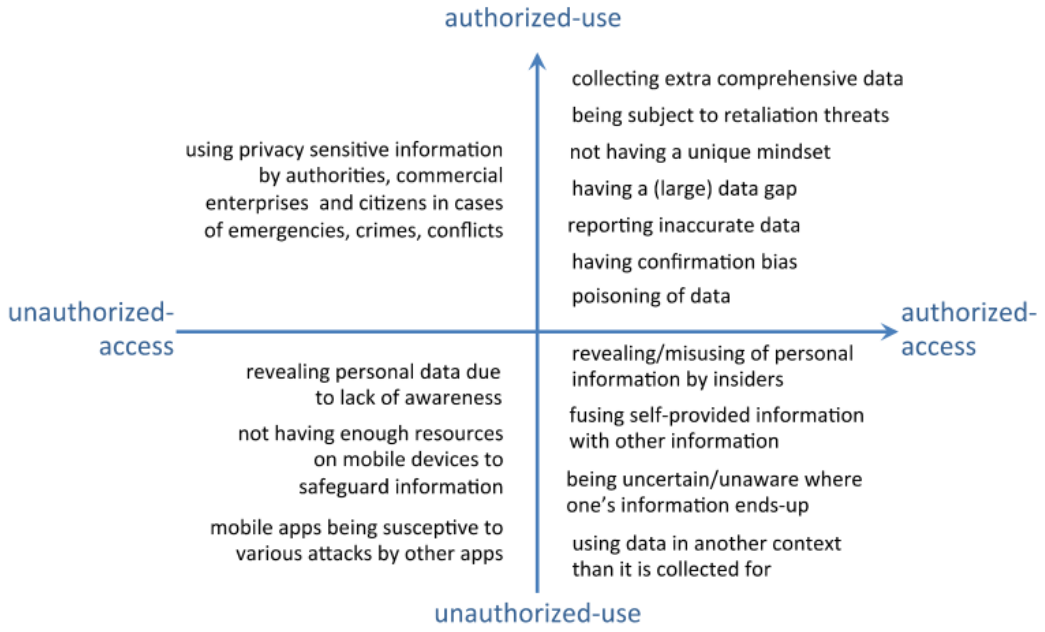

Figure 1: Four quadrants and examples (Source: Choenni et al., 2016)

The most known threats result from collected data that is illegally accessed and used (Choenni et al., 2016). Intruders illegitimately gain access to access and process the data.

Even if the access is formally authorized, Choennie et al. (2016) consider it as unauthorized when a user was unknowing, unaware of the impacts and unaware of the consequences. Users often make such wrong decisions if there is a lack of transparency or if the users earn immediate rewards.

Furthermore, malfunctioning of the device and malicious programs are threats to personal information. Even when data is accessed and used authorized, issues could occur. The data collected by users can be biased or inaccurate. Issues occur when decisions and services are based on this inaccurate or biased collected data.

When data is used in another context then it was originally collected for, it could conflict with transparency (Choenni et al., 2016). Even if the data is accessed authorized, the combination and aggregation of various data and usage by third parties could take place, without consent or awareness of the user (Barg & Choenni, 2013). On the contrary, Choenni et al. (2016) state that if the access of data is unauthorized it could still be used authorized. This could be the case if the usage of these unauthorized accessed data is of public interest or for safety reasons.

2.3.8. Location privacy and location-based services

A particular type of privacy is location privacy. Location privacy is defined as the ability to prevent other parties from learning one's current or past location (Beresford & Stajano, 2003). Beresford & Stajano (2003) argue that until recently, location privacy was a relatively unknown concept because people usually did not have access to exact information about the location of others. For that reason, people could not see any privacy implications in the disclosure of their location. However, with the rise of pervasive computing, the problem of location privacy changes completely (Beresford & Stajano, 2003).

Nowadays, services from third-party apps are very popular (Liang et al., 2017). These services collect location information from users and provide convenience. However, Liang et al. (2017) state that these services also threaten the privacy of users. The reason for this is that sensors within a device may release data without the user's awareness. For example, the released data can be used by malicious adversaries that threaten privacy (Grissa et al., 2017). Especially when location information is combined with other information or with frequency and timestamps, it could disclose information such as the behaviour of an individual, a religion or the health of the person.

Services that take the geographic location of an entity into account are called location-based services (Zhou, 2017). The term entity stands for the object that is triggering the location information, which could be a human or non-human (Junglas & Watson, 2008). Junglas & Watson (2008) state that within location-based service research, an important distinction is made between position-aware services and location-tracking services. They describe that position-aware services supply the user with personal location data, while location-tracking services provide information about the location of the user to other entities instead of to the user itself.

2.3.9. Four dimensions to measure usage of space.

Besides sharing location through handheld devices, presence can also be detected by sensors. According to Christensen, Melfi, Nordman, Rosenblum & Viera (2014), building occupancy is measured along the dimensions of resolution and accuracy.

There are many different types of sensors that can measure occupancy (Christensen et al., 2014). Christensen et al., (2014) state that some of these sensors only measure occupancy in a binary way, such as the PIR sensor that only measures if someone is present in a room, while other sensors also give additional information about the space such as the number of occupants. This difference of quality of the different of type sensors is called the resolution of occupancy by Christensen et al. (2014). A high-resolution sensor gives higher detailed information than a low-resolution sensor. They argue that the resolution of occupancy consists of three dimensions: spatial resolution, temporal resolution and occupant resolution. Spatial resolution relates to the structure of the building, for example by floors and rooms. Temporal resolution focuses on the smallest time span in which occupant and spatial resolution can be reported by a sensor.
Occupant resolution is a more complex type of resolution. As can be seen in figure 2, Christensen et al., (2014) define four levels of occupant knowledge resolution:

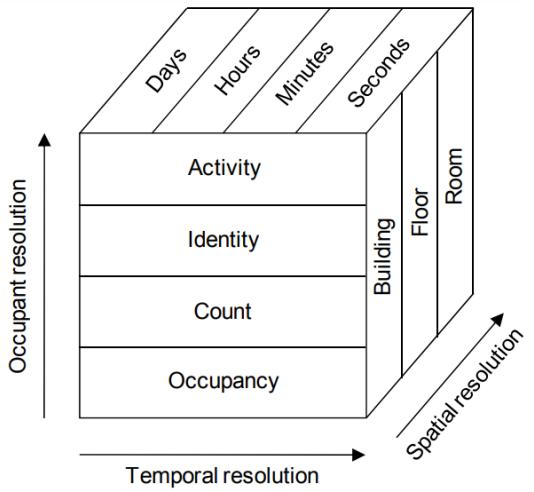

Figure 2: dimensions of space-use measurements (source: Christensen et al., 2014)

The first level of occupant knowledge resolution is occupancy. This only measures the relative error between the empty ground truth and the measured situation, which means if a person or object enters a room, the sensors will measure a difference from the ground truth and report that. Such a level of occupant knowledge resolution is a low-level resolution. A low-level resolution is acceptable if an incorrect decision is also acceptable.
Count is the second level of occupant knowledge resolution. At this level, the sensor measures how many people there are in a zone. An example of a sensor with high accuracy is a camera, which can count all the individuals (Chen, Jiang & Xie 2018). A CO^2-meter is less accurate and obtains a rough estimation of occupancy (Chen et al., 2018). According to Chen et al. (2018), every sensor has its own abilities and limitations.

The third level of occupant resolution is identity. This level focuses specifically on information about the identity of the occupant in the room. The sensors obtain information about the occupant and an algorithm attaches a label to the occupant, such as age or gender. The differences in accuracy, as mentioned above, also applies to these sensors. Activity is the fourth and last level of occupant resolution and this obtains information about what the occupants are doing at the measured location.

3. Methodology

Now that all relevant theories and concepts for this research are discussed in the theoretical framework, the methodology for the research is described. The methodology in this research consists of mixed components. The various methods in this thesis are a combination of research methods and pragmatic handling, whereby it is assumed that they complement each other to tackle the multifaceted subject in this research. This multidisciplinary subject does not lend itself in one particular method. The methods are related to the objectives and the methods could thus vary per objective. This section starts with a description of the case area. Thereafter, the strategy of the research will be explained, followed by the research approach. Next, the research design and the research instruments are discussed. The rationales for the choices made in this research are to be explained as well in this section. The limitations of the methods that come with them are also discussed. Last, statistics about the sample is given and the representativeness of the sample size is tested.

3.1. Case area and population

The Delft University of Technology was founded in 1842 and was originally located in the old city of Delft (Van der Hoeven, 2015). After the number of students had grown, it was necessary to relocate the buildings to a much larger site at the south of the city, in the Wippolder. The faculties moved to the new greenfield site during the 1960s and 1970s. The Campus was designed from a functionalist design along a linear axis of the Mekelweg and grew gradually to the current Campus. The campus map of TU Delft is shown in figure 3. The land-use area of TU Delft campus is 162 HA and in total, the campus consists of 54 buildings (TU Delft, 2020). The student population at the start of the academic year of 2019/2020 is 24,783, while the population of PhD students is 2,816. The number of scientific staff is 3,626 while the number of professional services is 2,446 people (TU Delft, 2020). A combination of these groups of users leads to almost 34,000 users of the Campus, which makes TU Delft the largest technical university in the Netherlands (TU Delft, 2020). On a regular basis, approximately 27,000 users are on campus per day.

The university offers a total of 49 education programmes, consisting of 16 bachelor's programmes and 33 master's programmes. Out of the 24,783 students, 5,931 students started in 2018. 5,519 students started in 2017 and 5,030 students started in 2016, 53% of the students studied a bachelor's programme, 45% studied a master's programme while 2% studied a bridging programme (TU Delft, 2019). In 2018, about 28% of the student population was female and 72% was male.

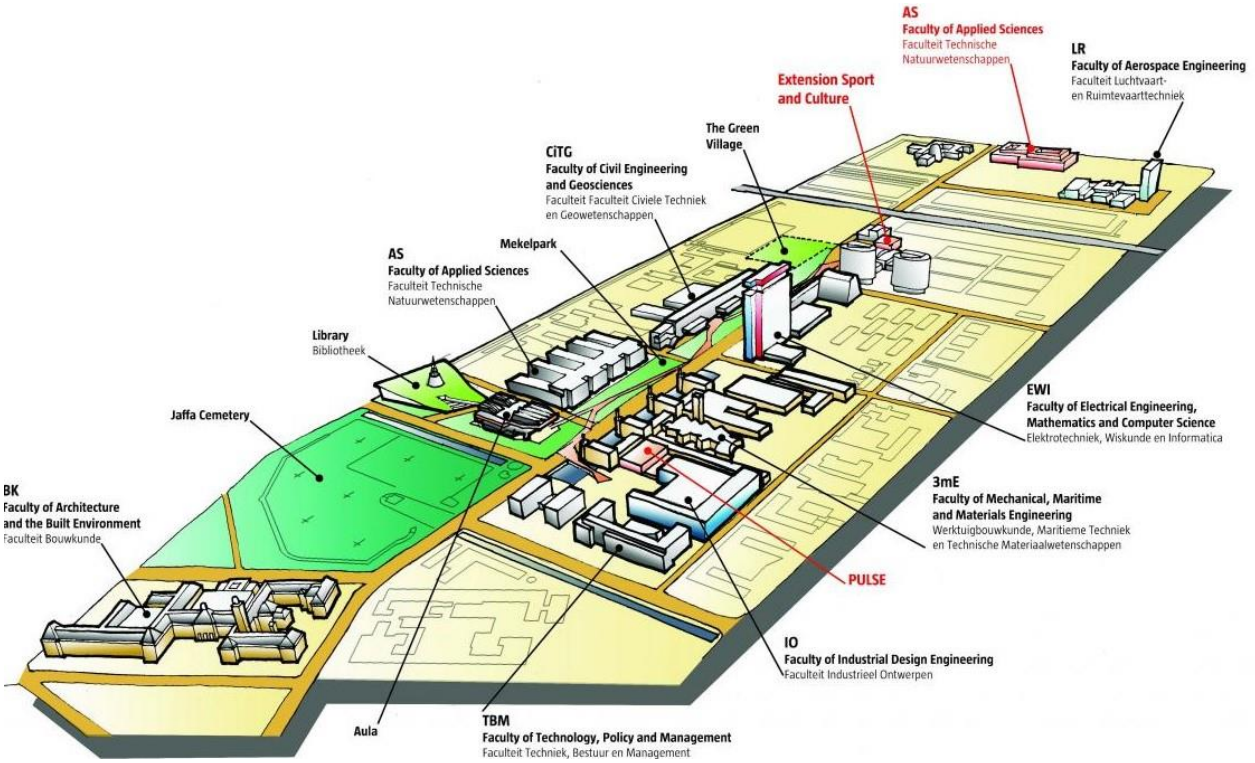

Figure 3 Campus map TU Delft (Source: Villares, 2016)

3.2. Research strategy

This thesis has a mixed-methods research strategy, which is a research strategy that combines both quantitative forms and qualitative forms of research (Bryman, 2014, p. 76). The rationality for this mixed-method strategy is that both methods can be integrated into a single project to complement each other (Creswell et al., 2007). The quantitative form could describe what happens in the perception of geographical data by campus users and the qualitative form focuses on more in-depth information about the current state of smart campus tools. Bryman (2012) presents several ways to combine quantitative and qualitative research. In this case, the specific way for the mixed method strategy is mostly characterised as “context”, which implies that the combination of the two research methods is rationalized in terms of a qualitative type of research that gives context for a survey (Bryman, 2012, p.633). This survey then couples the context with generalizable findings and relationships. Furthermore, the combination of mixed methods can be used for “instrument development” (Bryman, 2012, p.634). Hereby, the qualitative research method is employed to develop a questionnaire and scale items. E.g. questions in the survey could be narrowed down to receive more comprehensive answers.

3.3. Research approach and design

This study has a strong inductive approach, which means that new inferences are drawn out of the research, or in other words: new theory arises from observations (Bryman, 2012, p.26). This thesis’ approach can be seen as grounded theory. In grounded theory, which is an iterative process, concepts and theory are generated out of data (Bryman, 2012, p.387). In this process, data collection, analysis and eventual theory stand in a close relationship with each other.

This also applies to this survey since the second part of the research is based on the outcomes of the first part of the research. Furthermore, the outcomes of the second part of the research are again reflected on the first part of the research.

The research design in this mixed-method strategy is a cross-sectional design for both methods. A cross-sectional design involves more variables which are examined to find patterns, at a single point in time and in more than one case (Bryman, 2012, p.58). More than one case means a variety of examinations of the respondents. The research is conducted at a single point of time. Thus, the data is collected more or less simultaneously. The quantitative method will only be accessible for one month. A limitation of research of simultaneous data sampling is that it creates ambiguity about the direction of causality (Bryman, 2012. P.59). If a relationship is discovered, the researcher cannot be sure if this is a causal relationship. All that can be concluded is that there is a relationship between variables. However, it is not impossible, but within cross-sectional research, internal validity scores lower.

3.4. Research instruments

As there are various research strategies, various research instruments are also used within this thesis. At first, secondary scientific qualitative data is analysed. Secondary means that the analyst of this research did not play part in the data collection (Bryman, 2012. P.587). This secondary analysis mostly leads to a large volume of data. At second, this secondary qualitative data is complemented by an unstructured qualitative interview, which tends towards a consultation.

At third, a survey will be conducted to collect privacy perceptions of a sample of all the campus students. The survey is a self-completion questionnaire. A limitation of an unsupervised self-completion questionnaire could be that the respondents are able to interpret, which may lead to biased answers. Therefore, it is highly important to operationalize the questions as specific as possible. Originally, it was the intention to conduct the survey personally on campus with an iPad. The first few surveys are conducted this way. Very soon, however, the COVID-19 crisis began. Therefore, the survey is conducted via the internet. This survey will aim to complete objective II. The population of the TU Delft mostly consists of students. To keep the sample unified and to be able to generalize from the results, only the students are approached and researched. Hence, the staff of the TU Delft is not taken into account.

It is well known that surveys via the internet have a low response rate. To increase internet survey response rates, different strategies will be applied. At first, 24 boards of all the study associations at TU Delft, according to tudelft.nl, are contacted and asked to fill in the survey. Likewise, the boards are asked to distribute the link of the survey to their members. At second, individual students are written via email with the request to participate. With the help of a TU Delft email address, 1510 email addresses of individual students are manually and randomly extracted from the ‘people’ section in the email software. Afterwards, the individual students are contacted. The students are randomly selected by the initials in their email address. For example, 50 students of which the name starts with an A are contacted. Thereafter, 50 students of which the name starts with a B are contacted and so on until 1510 email addresses were extracted.

3.5. Software, data and research material

For this thesis, various software is used. For the design of the self-completion questionnaire, Qualtrics XM is used. This software is provided for free by the University of Utrecht. For the statistical analysis of the surveys, SPSS is used. The software is purchased via the University of Utrecht. No datasets are required for this thesis, other than the literature for the secondary analysis and the survey dataset, which is quantitative data that will be collected through the survey.

Most of the descriptive statistics of the survey will be presented using Microsoft Excel, Qualtrics-software and SPSS. The data is exported and prepared from Qualtrics to SPSS.

3.6. Operationalization

In this section, the link is established between the concepts of the theory and the themes that are to be found in the survey. The operationalization of the secondary analysis is presented within the secondary analysis chapter itself.

Every theme in the survey consists of a variety of questions. As stated earlier in this methodology chapter, the survey is a digital unsupervised self-completion questionnaire. The design of the questionnaire needs to be easy to follow and easy to answer since there is no interviewer (Bryman, 2012, p.233). This means that questionnaires have fewer open questions and more closed questions that are easier to answer. The design of the questionnaires should be minimized in order to prevent failures of the respondents and the questionnaires need to be as short as possible to reduce the risk of respondent fatigue (Bryman, 2012, p.233). Moreover, it might be possible that an individual respondent interprets questions different from another respondent, which results in incorrect answers. Therefore, it is required to formulate the questions as specific as possible to prevent the respondent from interpretation. To get more familiar with survey software and to test how the respondents answer, a pilot survey was held amongst 4 students of TU Delft.

Table 1: schematic overview of questionnaire

Theme	Question	Operationalization	Question type
Respondents Background	Q1	Age	Multiple choice
	Q2	Gender	Multiple choice
	Q3	Respondent's university	Multiple choice
	Q4	Type of degree	Multiple choice
	Q5	Study	Open
	Q6	Year of start study	Multiple choice
Activities on campus	Q7	Type of activity	Checkboxes
	Q8	Frequency of visits on campus	Multiple choice
	Q9	Detectable devices on campus	Checkboxes
Privacy and knowledge of privacy in general	Q10	Concerns about location information per organisation	Likert-scale
	Q11	Familiarity of content	Likert-scale
	Q12	Ability to control personal data	Likert-scale
Smart campus tools	Q13	Methods of detection on campus	Checkboxes
	Q14	Usage of smart campus tools	Checkboxes

Current privacy perception on campus	Q15	Sharing location information	Likert-scale
	Q16	Awareness of content of shared data	Likert-scale
	Q17	Understanding of data handling	Likert-scale
	Q18	Ability to control location data on campus	Likert-scale
	Q19	Perception of potential risk	Likert-scale
	Q20	Selectiveness in sharing location data	Dichotomous
	Q21	Explanation of selectiveness	Open
	Q22	Perception of protection of personal data on campus	Likert-scale
Attitude towards smart campus	Q23	Comfortability about usage of personal data on campus	Likert-scale
	Q24	Acceptability of being tracked	Likert-scale
	Q25	Commercial reuse of location information	Likert-scale
	Q26	Commercial involvement in smart campus	Likert-scale
	Q27	Presence disclosure via cameras	Likert-scale
	Q28	Presence disclosure via sensors	Likert-scale
	Q29	Collection of personal information via Wi-Fi	Likert-scale
	Q30	Usage of Quantified Student application	Likert-scale
	Q31	Disclosure of location information for functioning of campus	Likert-scale
Future perception of campus	Q32	Expected effort of protecting location data	Likert-scale
	Q33	Why increasing effort	Open
	Q34	Why not increasing effort	Open
	Q35	Desirability of integrated smart campus	Likert-scale
	Q36	Perception of ability to control in 5 years	Likert-scale
	Q37	Expectations of benefits of data sharing	Likert-scale
	Q38	Best safeguard for personal information	Likert-scale

In table 1, a schematic overview is presented that shows what topics of the operationalization are included per theme. These topics are put into 38 different questions. The themes are composed, based on the theoretical framework. These 7 themes are identified because it is assumed that together they measure the students' privacy perception on campus. Furthermore, the type of question is also specified in the scheme.

As shown in the scheme, the survey first focuses on the background information from the respondents and their activities on campus. Here, the age, gender, the university where the respondent is enrolled, the type of degree of the respondents' study, the name of the study and the starting year of the study is questioned. These questions are included to research how the sample of the survey is distributed over the population and thus if the sample is representative. Within the second theme activities, the type of activities, the frequency of visits to the university and the usage of devices on campus is questioned. This theme is used to measure what most students do on campus and if the campus is indeed a city in miniature, as described in the theoretical framework and introduction, or if it is a monofunctional space for education.

Afterwards, the students are questioned about their general knowledge of privacy. Herewith, the respondents are asked how familiar they are with regulations and privacy policies of the campus and campus' organisations.

Furthermore, they are asked how concerned they are about their privacy at the government, the university and commercial parties. The last question in this theme concerns the respondent's ability to have control about their location data, online data, data from campus-services and offline data, such as conversations. These questions are included to research the overall perception of privacy in terms of knowledge, awareness and concerns of data in general and within different organisations. This overall perception also gives weight on the perception of privacy on campus since this can be compared. Herewith, the perspective on privacy regarding the university is also questioned.

Thereafter, the respondents are asked whether they use smart campus tools and how they think their presence can be tracked on campus. This theme is composed with the help of the secondary analysis about smart campus tools and the way users think they can be detected on campus, which can be compared to the real situation on campus.

Then, the survey aims to measure current privacy concerns and the perception of privacy on the campus. This theme consists of 8 questions. The first 5 questions are Likert-scale questions to measure the respondent's perception. This starts with a question if the respondent knows that they share data at all. Then, they are asked if they know what data they share and if they understand how their data is processed on campus. This is followed by the question how they feel about the ability to control their data on campus. The next question focuses on the perceived potential risk of the respondents of losing their data or misuse of their data on campus. To the end of this theme, three questions remain. Two questions ask the respondents if they are selective in sharing their data, and if so, a question asks: how? The last question questions their overall perception of the protection of their data on campus. These questions consist of a combination of the processed privacy theory. It is assumed that a combination of privacy concerns, privacy awareness, privacy cognition, perceived ability to have control over personal data, perceived risk of losing or misuse of information and privacy behaviour determine the perception of privacy and the perspective on data within the campus.

After that part, the attitude of respondents is measured about smart campus tools that are already in use or tools that are in a pilot phase. In this theme, these smart campus tools are not per se in use on campus at TU Delft. The smart campus tools that are found in the secondary analysis are presented with Likert-scale questions. Furthermore, the respondents are asked if they are willing to share their data if this makes the campus more efficient and if they are willing to share data for other benefits, specified per smart campus tool. These questions again are a combination of the outcomes of the secondary literature and the assumption that people want to share data if they expect the return to be beneficial, as discussed in the theoretical framework.

Finally, the future and expected perceptions of location privacy on a smart campus are researched. Hereby, it is assumed that throughout the survey, the respondents are better informed about what a smart campus is. The respondents presumably have an opinion about the desirability of a smart campus. They are questioned if they expect that the effort for protection of their personal data in 5 years increases or decreases. This question comes along with two open questions where they can fill in why they expect to see a change in their effort. These questions are of course highly important to answer the research question and to achieve objective IV.

The last question asks what the respondents think is the best safeguard for personal data on a smart campus. Although this is not an answer to the research question, the outcome could be useful for the chapter of the smart city design.

3.7. Sample size

For the survey about the perception of users on campus about the use of data on the campus, the focus will be on the students. A sample of all the students of TU Delft will be asked to participate in the survey. As stated in section 3.4 Research instruments, the email addresses are extracted from TU Delft email software and the email addresses are randomly chosen, based on the first letter of their name. As described in the case description, the population size for the survey is 24,783. The margin of error is aimed at 8% and at any rate below 10%. The confidence level is aimed at 95%, which implies that the results from the sample size are the same as in 95% of other possible samples. The students of TU Delft are considered as a relatively homogeneous population because the difference in age is small and they all have the same education level. (Bryman, 2012. p. 200) Therefore, the amount of variation is smaller which is why the sample can be smaller.

Due to the nature of the procedure of the sample selection, the response rate for the survey is expected to be very low (Bryman, 2012. p.185). Furthermore, the length of the survey and the fact that the survey is a self-completion questionnaire will have the result that people do not finish the survey (Bryman, 2012, p.186). The expectations for the response rate are approximately 10%. This expectation is based on the pilot survey. Another reason why this response rate is expected to be low is the fact that there are no material incentives for the respondent. The respondents should participate in the survey out of interest and curiosity. Thereby, the survey is conducted and administered via the internet and is not supervised, which also affects the response rate (Bryman, 2012 p.188).

If the margin of error is 8% and the confidence level is 95%, it means that the sample size should be 151 (SurveyMonkey, 2020). If the margin of error is 9% or 10% with a confidence level of 95%, it means that the sample size should be respectively 119 and 96.

Based on a sample size of 151, this results in a total of 1,510 students that should be invited to take part in the survey. However, the study associations are also contacted and it is unknown what their contribution was to the response rate. Most probably, the estimated response rate was lower for individually contacted students

These students are invited according to a probability sample. A probability sample suggests that the selection of the sample size is done randomly and systematically (Bryman, 2012. p.187). Because of the random selection, each unit has the same chance of being selected. The sample is unbiased. It is generally assumed that random selection is more likely to be representative to the population than a sample that has not been selected using a random selection method. The selection in this research is random since the students are selected based on their initials. However, this type of selection is random to a certain extent, since names and thereby initials of students probably relate to their ethnic background or gender.

3.8. Sample representativeness

In this part, there will be analysed whether the sample of respondents that filled in the survey is representative for the whole student population at TU Delft. If the sample is representative, the sample data will be close to corresponding to the population data (Bryman, 2012. p.200). In other words, if the sample is representative, the findings in the survey could then be generalized to the whole of the student population at TU Delft. As a result of the low response rate, it may be the case that there is a selective group of nonrespondents. Thus, these tests research if this is the case. This test solely calculates the representativeness of the sample for three variables. Hereby, the profile of students that agreed to participate in the survey cannot be considered. Therefore, the possibility that the invitation for the survey is mostly accepted by students that have a better perception of privacy could not be excluded. This limitation should be considered in regard to the representativeness of the sample.

Samples contain less information than the population. So, estimates from this sample will have some uncertainty. In this thesis, the uncertainty level is 7.90% for a population of 24,783 and a sample size of 153 students. Hereby, the confidence level is 95%. The results show, however, that the number of respondents gradually decreases when the survey proceeds. Therefore, the uncertainty level rises per question. The last question is answered by 102 respondents. This means that the margin of error is at most 9.68%. At the end of the survey, this is less consequential since the questions are more exploratory and open. In table 2, the n-value and the number of missing values can be seen per question. *-questions are questions with selection criteria. Therefore, these questions are not included. The decline in number of answered questions is due to the medium on which the survey is conducted, the fact that the survey is unsupervised and the duration of the survey.

Table 2: response rate per question

Question	N-value	Missing	Question	N-value	Missing
Introduction	153	0			
Q1	148	5	Q20	115	38
Q2	148	5	Q21	*	n/a
Q3	147	6	Q22	114	39
Q4	147	6	Q23	107	46
Q5	146	7	Q24	107	46
Q6	148	5	Q25	107	46
Q7	148	5	Q26	107	46
Q8	145	8	Q27	107	46
Q9	145	8	Q28	106	47
Q10	125	28	Q29	106	47
Q11	125	28	Q30	106	47
Q12	124	29	Q31	106	47
Q13	120	33	Q32	106	47
Q14	119	34	Q33	*	n/a
Q15	116	37	Q34	*	n/a
Q16	114	39	Q35	105	48
Q17	115	38	Q36	105	48
Q18	115	38	Q37	104	49
Q19	115	38	Q38	102	51

To test if a categorical variable of the sample is representative, a chi-square test is a possibility to calculate the goodness of fit (Preacher, 2001). The deviation of nominal variables of the sample will be compared with the statistics from the student population at TU Delft. The variables that will be tested with the chi-square test are the gender of the students, the type of degree of their study and the faculty to which their study belongs. All tests are calculated twice, to verify the outcomes. At first, the test is calculated manually and at second, the test is calculated with software from Preacher (2001).

It is not possible to test the representativeness of the sample for the age of the students, since the TU Delft has not published data about students' age. Besides that, the starting year of the students cannot be tested with the chi-square goodness of fit test with the current data of the University of Delft. The problem with the data from TU Delft is that only data is published about new registrations at the university. The result is that this data cannot be tested to the data in this thesis. This can be explained by an example: if a student started at TU Delft in the year 2015 and he started his master's program in 2019, the student is not new to the university. However, according to the data in this survey, the student started in 2019.

The chi-square test is also not performed for the studies that are followed by the students. Mathematically, this is not very interesting with a response of N=146. Because of the high DF value that results from the wide variety of possible studies at TU Delft, the H0 hypothesis will be accepted. Therefore, the data of the studies is aggregated to the faculty of which the study is part of.

At first, the chi-square test for gender is performed. Hereby, the ratio of male/female students in the sample is compared to the ratio of male/female students at TU Delft. As can be seen in table 3, gender is unequally distributed at TU Delft. Men outnumber women more than 2.5 times. On the other hand, gender is almost equally distributed in the survey. If the survey would have followed the actual distribution, the student sample would have been quite different. For this chi-square test, a significance level of 0.05 is chosen.

The result of the chi-square test for goodness of fit is $X^2 = 31.13324901$. However, even more important is the result that chi-square is significant (p=0.00001). This implies that the H_0-hypothesis is rejected and that the distribution in the student sample is not representative for the student population regarding the variable gender.

Table 3: Chi-square test for goodness of fit on gender

Absolute			
	Student population	**Student sample**	**Expected in sample**
Male	17,775	76	106
Female	6,928	72	42
Total	24,703	148	148
In percentage			
	Student population	**Student sample**	
Male	71.95%	51.35%	
Female	28.05%	48.65%	
Total	100.00%	100.00%	

At second, the chi-square test for the types of degrees are calculated. In this test, the distribution of the types of degrees in the sample is compared to the distribution in types of degrees in the student population. As shown in table 4, most of the students at TU Delft do study for a bachelor's type of degree. The other students mostly study for a master's type of degree. Less than 2% follows a bridging program. In the student sample, this distribution is somewhat similar. For the chi-square test, the value of the students that study a bridging program could be problematic because the value is below 5. In the chi-square test, it is assumed that the expected values are above 5 (Preacher, 2001). However, the chi-square test is still performed and results in a value of $X^2 = 0.016114631$. With a DF value of 2, this value is below 5.99 and the H_o is rejected if the p-value is not significant. The p-value = 0.99197506 and is not significant with a significance level of 0.05. This means that regarding the type of study, the student sample is representative for the student population. If the bridging-students are not taken into account in the test to avoid expected values below 5, the results are $X^2 = 0.002$, with p-value = 0. 0.96460149. Without the bridging students, the student sample is still representative for the student population.

Table 4: Chi-square test for goodness of fit on type of study

Absolute			
	Student population	**Student sample**	**Expected in sample**
Bachelor's	13081	78	78
Master's	11151	66	66
bridging	471	3	3
Total	24703	147	147
In percentage			
	Student population	**Student sample**	
Bachelor's	52.95%	53.06%	
Master's	45.14%	44.90%	
Bridging	1.91%	2.04%	
Total	100.00%	100.00%	

The third and last chi-square test for goodness of fit that is performed concerns the variable faculty. As stated earlier, the studies are aggregated to the faculty to which the study belongs. The n-value is 144 since 2 studies could not be aggregated to a specific faculty. The distribution is shown in table 5. Almost 20% of the students at TU Delft are attached to the faculty 3ME, which is the faculty of mechanical, maritime and materials engineering. In the student sample, this faculty is also most represented. TBM, which is the faculty of technology, policy and management, is lowest represented at TU Delft. This also applies to the sample. The result of the chi-square test is $X^2 = 4.695933229$. With a DF-value of 7, this is below 14.07. Thereby, the p-value = 0.6970131. With a significance level of 0.05, the H_o-hypothesis is rejected. This implies that the distribution of the student sample is representative for the distribution of the student population.

Table 5: Chi-square test for goodness of fit for the faculty of the students

Absolute			
	Student population	Student sample	expected in sample
3ME	4866	27	28
BK	2806	20	16
CITG	3644	19	21
EWI	4024	21	23
IO	1964	13	11
LR	2642	14	15
TBM	1613	6	9
TNW	3144	24	18
Total	24703	144	144
In percentage			
	Student population	Student sample	
3ME	19.70%	18.75%	
BK	11.36%	13.89%	
CITG	14.75%	13.19%	
EWI	16.29%	14.58%	
IO	7.95%	9.03%	
LR	10.70%	9.72%	
TBM	6.53%	4.17%	
TNW	12.73%	16.67%	
Total	100.00%	100.00%	

4. Analysis

4.1. Secondary analysis

To be able to analyse privacy on TU Delft Campus, both the actual state of privacy and the perceived privacy are researched. The determination of the actual state of privacy on campus falls under objective I and III of this thesis. In this first section of the analysis, the current state of the development of the smart campus will be described as well as the status of privacy for users on campus through a secondary analysis. To do so, the development of campuses at international universities and the Netherlands will be discussed. Ultimately, the campus of TU Delft will be discussed. The tools that are used on these various campuses are presented and described. The section follows the scaling down of international campuses to Dutch campuses to the TU Delft campus.

This section will elaborate on what type of information is used in smart campus tools by universities, how the information is used, what technologies are used and for what purpose information is used. Different sources are used in this section to research the current state of privacy on campus. The main sources are the book Smart Campus Tools 2.0: An international comparison (2018), the book Smart Campus Tools: An exploration at Dutch universities and lessons from other sectors (2016), a consultation with the co-author of these books Bart Valks and an online interview at tudelft.nl. Within the books of smart campus tools, the user needs and requirements are not directly researched. This is mostly examined by the campus management from the researched university.
Bart Valks is both a TU Delft campus manager and a PhD researcher at the Faculty of Architecture and the Built Environment. In his PhD on 'Smart campus tools', he researches how universities can make more effective and efficient use of their real estate and how technology can support them to achieve this (BOSS, n.d.).

The main purposes, for which information is used within the smart campus, are divided into three groups (Valks et al., 2018. p.30). The first group is the purpose to save energy, the second group is to optimize usage of space and the third group is to support the users of the campus. To achieve this, there are smart campus tools.

These tools are most of the time for education spaces and are periodically monitored through the comparison between the predicted occupancy and the actually counted occupancy. Some universities determine the occupancy with the help of Wi-Fi tracking. Thereafter, the periods are compared to the year before to improve the timetabling process.

For study spaces, most universities do not monitor the occupancy. However, universities provide their students with tools to find available desktop PCs and to book available rooms. Thereby, they also give students more and more access to non-booked classrooms and meeting rooms.

At universities, a wide variety of techniques and sensors are used to measure. These techniques are radio-frequency identification (RFID), Wi-Fi tracking, Bluetooth, Infrared, Cameras, Ultra-wideband, Wearable devices, and carbon dioxide detectors (Valks et al., 2016. p. 34). Within these techniques, there are several applications to use these techniques (Valks, 2020). For example, Within Wi-Fi tracking, the existing networks can be tracked.

This can be tracked with gathering information about which devices are connected to the network, how long these devices are connected to the network and the location of these connected devices. The location of the connected devices is estimated with the help of received signal strength indication values (RSSI). The results of the estimated location of the devices, based on the Wi-Fi tracking, are used to measure occupancy or usage of spaces. When the devices are analysed with Wi-Fi tracking and linked to other data, it is feasible to give users a label such as what courses they do. Another application for Wi-Fi tracking is to create an entirely new network of scanners and sensors to track devices for analysing occupancy and usage of space. With Wi-Fi tracking, it is even possible to track devices that are not connected because these devices still send out messages to the Wi-Fi receiver (Musa & Eriksson, 2012).

4.1.1. Current Smart Campus Tools on international universities

Valks, Arkesteijn & den Heijer (2019) conducted a survey and this resulted in 12 researched international universities. According to Valks et al., four of these researched universities did not have any smart campus tools in use or in development, while at the other 8 universities the functions of the smart tools are highly diverse. This secondary analysis uses these 8 international campuses. The data that is gathered per university is the following:

- The name of the university.
- The phase of the smart campus tools.
- The scale of the smart campus development in buildings and m².
- The “why-question”, which concerns the motivation why the university has chosen these smart tools.
- The “what-question”, which concerns the type of data that is collected with the help of smart tools. The type of data will be explained according to the typology of Christensen et al.
- The “how-question”, which concerns the specific methods that measure the data from the “what-question”.
- The people that have access to the data that is collected by the help of the smart tools.

Besides these parameters, the timespan that the data refreshes and privacy measurements are also included, if available.

Aarhus University ,Denmark	
Scale	16 buildings, 40,000 m²
Phase	Design brief
Why	To help find available study places.
What	Occupancy and identity of users. Real-time information on room or floor level to search for available places.
How	iBeacons measures the number of occupants by letting devices connect with Bluetooth.
Privacy	Users need to give agreement for usage of an app to give permission to collect the required data.
Access to tool	Open Access

Saïd Business School, United Kingdom	
Scale	1 building, 840 m²
Phase	Future implementation
Why	A solution that shows the entrepreneurs who are currently in the building and what their field of interest is.
What	Identity of users
How	Access gates that register if a person has entered the building
Privacy	People need to enable or disable the service.
Access to tool	Users' access

Technical University of Denmark, Denmark	
Scale	1 building, 35,000 m²
Phase	Pilot
Why	First, the university wants to make the library smart as a pilot and after the pilot, the complete campus must be made smart. Among others: indoor climate, lighting and to help students find a study place.
What	Realtime measurements of frequency, occupancy and activity. Later if possible, identity.
How	Sensortag placed under the chair which measures movement, temperature, humidity. Cameras to measure the number of users in a square, communicate with other cameras that monitor other squares.
Privacy	Users need to give agreement for usage of an app to give permission to collect the required data.
Access to tool	Open Access

University of Leuven, Belgium	
Scale	10 buildings, 28,785 m²
Phase	Implementation
Why	To give students an application for the availability of study places across the campus.
What	Occupancy and identity of users. Number of registered users that are present at a location is measured with a refresh rate of a few minutes.
How	Access control systems with campus cards. Each user is counted.
Privacy	
Access to tool	Open Access

Carnegie Mellon University, United States	
Scale	1 building, 13,470 m²
Phase	Research
Why	To set up a living laboratory for Internet of Things applications, with special focus on privacy and security in the development. This development is funded by Google. The goals are optimization of CO^2 and reducing cost of HVAC systems
What	Occupancy and Identity of users. For individual offices, the presence of users in offices is measured. Therefore, the system requires to know who belongs to which office and the system needs real-time user data. Furthermore, users' wellbeing in a room is measured. Users can request data about temperature and energy usage.

How	Wi-Fi measurement to measure specific users on specific locations. Users' wellbeing is measured with a thermostat that measures temperature and CO^2.
Privacy	
Access to tool	No open access, information only in the system for offices. The wellbeing-function is accessible for users.

Oxford University, United Kingdom	
Scale	1 building, n/a m^2
Phase	Design brief
Why	For more efficient use of space, and to share research and teaching space. University is considering investing in a moveable sensor infrastructure for occasional space utilization measurements to evaluate demands for additional spaces.
What	Frequency and occupancy of users in teaching space. In office space, each desk is measured. In meeting rooms only if there is a user present or not. The data is only reported over a longer period
How	Passive Infrared sensors that register if a user passes through.
Privacy	
Access to tool	Only campus managers have access

Cambridge University, United Kingdom	
Scale	206 spaces, n/a m^2
Phase	Implementation
Why	There are many different buildings and students with different needs. Therefore, Spacefinder is developed, which provides an interface to navigate through all the buildings to find study places.
What	No space-use measurements.
How	
Privacy	
Access to tool	

Sheffield Hallam University, United Kingdom	
Scale	5 buildings, n/a m^2
Phase	Pilot
Why	Monitor teaching space on campus, in order to inform decision-making on its estates' masterplan and to improve timetables. Academics tend to overbook spaces, tools to penalize non-used bookings.
What	Frequency, occupancy and identity of users with real-time measurements.
How	Via reservation systems and Wi-Fi-measurements. The number of people is monitored. Actively via connections and passively via connection attempts on a certain time at a certain place. Thereafter, an algorithm pairs the devices to the person to which it belongs.
Privacy	
Access to tool	Campus management and support staff have access.

ÉPF de Lausanne, ETH Zurich, Reading University and Ulster University are the universities that do not have any smart campus tools in use or development. As stated earlier, the smart campus tools at international universities vary widely. Moreover, all tools are still in a preliminary phase.

5 out of the 8 universities measure the identity of the users, while the Technical University of Denmark also measures the type of activity. For the first three described universities, the privacy settings are known. These users can give permission to be tracked or they can enable or disable the data collection. The type of sensors also differs, Sheffield Hallam University and Carnegie Mellon University both use Wi-Fi measurements while Saïd Business School and KU Leuven both use RFID. Oxford University and Technical University of Denmark makes use of Infrared sensors while Aarhus University measures via Bluetooth. At most of these universities, the data is openly accessible and presented real-time to the user.

4.1.2. Current Smart Campus Tools in the Netherlands

For the secondary analysis of smart campus tools at Dutch universities, another 8 universities, which all use at least one smart campus tool, are presented in a similar way as the international universities. Valks et al. (2019) researched 14 universities. This secondary analysis uses only 8 universities since for these universities, two studies are conducted, both in 2016 and 2019. The first 7 universities are issued in this section and TU Delft is explained in the following section.

In contrast to the international universities, Dutch universities have a far more unified approach than international universities. This Dutch approach focuses on monitoring space use or it focuses on supporting users through a combination of finding study places, room bookings, and/or navigation. Even though smart campus tools are still in a phase of development on Dutch campuses, it could be said that Dutch universities are often further in this development than international universities.

Eindhoven University of Technology	
Scale	213,000 m²
Phase	Implementation
Why	A strong increase of students led to more students per M². A uniform system for reservations and findability of available spaces should help to achieve this.
What	Frequency is determined through the comparison of the duration of reservations and the maximum available hours for the space. In one building, there is a pilot with sensors that can determine an early leave or a no-show. Users can real-time see if a space is booked or not.
How	Reservations are made via the Planon reservation system. Presence in the meeting rooms is detected via infrared sensors that are connected to the lightning.
Privacy	
Access to tool	Students and employees have access to information that shows whether a room is booked or not. Secretaries have access to the reservations.

University of Amsterdam	
Scale	6 buildings, 105,184 m²
Phase	Expansion
Why	To visualize study places and project rooms and to give students more access to classrooms.

What	Occupancy is measured for PC spaces; frequency is measured for education spaces and project rooms. This is both done real-time.
How	The usage of desktop PCs is logged in order to show occupancy per workplace. For education spaces and project rooms, booking data from the reservation systems is used.
Privacy	
Access to tool	Location of study places and project rooms is visible to anyone; room bookings are only possible for employees and students.

Vrije Universiteit Amsterdam	
Scale	7 buildings, 276,484 m²
Phase	Implementation
Why	Optimization of space use and supporting the user. To show availability of education spaces and to display occupancy of PC spaces.
What	For PC spaces, the occupancy is shown. For education spaces and project rooms, the frequency is shown. Real-time.
How	Booking data should show whether an education space or project room is in use or not. PC login data shows if a PC space is occupied or not.
Privacy	
Access to tool	Only persons with a VUlogin have access.

Wageningen University	
Scale	6 buildings, 21,000 m²
Phase	Implementation
Why	To research how efficient the buildings are actually used and to optimize usage of m². This research should be done with the help of big data through the measurement of students to understand the use of education spaces.
What	Frequency, occupancy and Identity. An indication of the occupation is given for a certain space. The data is near real-time.
How	Via Wi-Fi the location of devices is determined. An algorithm determines if multiple devices belong to one user. Thereafter, the number of users is determined.
Privacy	To guarantee privacy, the IP addresses are anonymized every day in a different way.
Access to tool	Only available for managers and support of the campus.

University of Utrecht	
Scale	2 buildings, n/a m²
Phase	Pilot
Why	To get insight into frequency and occupancy rates of education spaces to improve space use.
What	Frequency and occupancy. The number of devices on a certain location is measured. Thereafter, an algorithm converts this into the number of users.
How	Via Wi-Fi, the attempts to connect to the network are measured as well as the number of connected devices. Based on the signal strength, the location is estimated.
Privacy	
Access to tool	Managers and support from the project management team.

Tilburg University	
Scale	2 buildings, 5,000 m²
Phase	Design
Why	Provide students a user-friendly tool to book meeting rooms. Besides that, the university wants to increase the frequency rate and findability of meeting rooms.
What	Yet to decide. However, frequency and occupancy are expected.
How	Sensors yet to decide. The sensors need to measure the space use real-time.
Privacy	
Access to tool	Unknown

Twente University	
Scale	5 buildings, 5,360 m²
Phase	Research
Why	Support interactive, project-driven learning and a chance of planning. A lecturer can choose real-time the needed space instead of planning in advance.
What	Frequency, occupancy & Identity. The number of connected devices is measured. This number is converted into users with the help of Eduroam data.
How	Wi-Fi measures the registered and unregistered MAC addresses. Every 6 minutes.
Privacy	
Access to tool	Support staff have access.

The scale of Eindhoven University of Technology, University of Amsterdam and Vrije Universiteit Amsterdam is worth noticing, their smart campus tools cover a huge scale compared to other Dutch universities and other international universities. Besides that, in most cases, frequency and occupancy are measured. Twente University and Wageningen University also measure identity through coupling users to their Wi-Fi signal. Furthermore, booking systems, sensors and cameras are used at Dutch universities. The smart campus tools are mainly focused on efficient use of space and student support.

A notable difference between Dutch universities and international universities is who has access to the tool. At Dutch universities, mostly support staff or campus managers have access to the data, while tools at international universities are mostly openly accessible. Hence, the data of campus tools in Dutch universities is often not open. In most cases, the tools on Dutch universities are based for reporting and monitoring efficiency of space-use, while international smart campus tools are often meant for both users and support staff.

4.1.3. Current Smart Campus Tools in Delft

Now that the international and Dutch universities are compared and analysed in terms of their smart campus tools, the TU Delft is analysed. The next two tables show that at TU Delft there are two main smart campus tools in use: Mapiq and a pilot for a tool for education spaces, which is still unnamed. For the Mapiq tool, frequency and occupancy are measured through the combination of infrared sensors and a reservation system. Only a few project members and two further unspecified persons from the faculty have access to historical data about the reservations and the occupancy of workplaces. In the pilot, frequency, occupancy and identity are measured real-time. These measurements are taken through a combination of Wi-Fi data and a reservation system. The Wi-Fi registers the connection attempts and the number on connected devices. The location is estimated based on the signal strength. The identity of the user is anonymised, before it is sent to the cloud.

Delft University of Technology: Mapiq	
Scale	2 buildings; the library and the faculty of Industrial Design Engineering (IO), 26,000 m²
Phase	Implementation
Why	TU Delft wants to support user activities and stimulate collaboration by enabling reservation of project rooms and by offering information that concern amenities in the library.
What	Frequency and occupancy. The occupancy of 100 workplaces is shown real-time. Meeting rooms are monitored via reservations and via sensors to see if they are indeed in use.
How	The main data source is reservations from the reservation system. Besides that, 100 infrared sensors have been added on workplaces and 10 infrared sensors have been added on meeting rooms, they both measure activity.
Privacy	
Access to tool	Open access: Availability, location of each space and blueprints are visible for everyone. Reservations can only be made by students and employees. Only support staff can access the backend of the booking tool. Specific individuals can access the reporting function that shows the data as far back as possible.

Delft University of Technology: education spaces	
Scale	1 building; the faculty of Mechanical, Maritime and Materials Engineering (3mE), 25,000 m²
Phase	Pilot
Why	Better insight into the use of facilities on campus and to optimize usage of M². Growing student population which puts pressure on education spaces. To monitor the usage and to schedule more efficiently in the future.
What	Frequency, occupancy and identity. The number of connected devices in a building at a certain time is measured. An algorithm converts this number of connected devices to the number of people. On-site, the Wi-Fi data is anonymized. Furthermore, if anyone is able to deanonymize the data, the user can never be tracked for longer than one day since a different encryption is used. All data is real-time. In lectures, the frequency and occupancy are shown. The reports show data per period.
How	The Wi-Fi registers both the connection attempts as the connected devices. The location is estimated based on the strength of the signal. In addition, data from the reservation system is used.
Privacy	
Access to tool	Access by support and managers.

This secondary analysis shows that TU Delft uses smart campus tools on a relatively small scale, compared to other Dutch universities as University of Amsterdam or University of Utrecht. Valks indicates that at this moment, TU Delft is considering if they want to implement a system to monitor the usage of education rooms (B. Valks, personal communication, March 9, 2020). Within this process of consideration, there is a major part focused on how the campus should be organized.

If efficiency for usage of education rooms need to be improved, other organizational structures such as schedulers also need to be organized in a different way, since these organizational structures are dependent on each other.

According to Valks, the concept of smart on the campus of TU Delft may be seen as a collective term (B. Valks, personal communication, March 9, 2020). The smart campus consists of a variety of solutions for a variety of problems. However, it is not completely integrated into a single system. In the future, it will probably move towards a more integrated system, he thinks. This integration is already in development, although it is unknown how far this integration will reach. Valks mentions that there are companies that work with architecture such as data lakes or an intermediate layer with information, which various systems can access. Herewith, the data is then centralized. Within the campus of TU Delft, there is no such integration or data lake in development.

Currently, the Wi-Fi data of the Eduroam-network at TU Delft is available for researchers of the university, such as Ph.D. students and their supervisors or individual researchers (TU Delft Library, 2016). For this Wi-Fi data, there are directives for when this data can be used for research and for what purposes. The content of this Wi-Fi data are Wi-Fi logs that cover all indoor space and even large outdoor spaces on campus (Griffioen et al., 2017). Griffioen et al. (2017) define that Wi-Fi logs are individual connections of mobile devices. They state that long-term continuous collection of connections allows it to track devices. All the connections in the network are logged at regular intervals of 5 minutes and are stored in a database. In their research, Griffioen et al. (2017) were able to map movement patterns between buildings and in building parts for the whole campus.

Sennet (2018) stated that the purposes in a smart city are very important for the sense of a smart city, while Zuboff (2019) stated that the label ‘smart’ is used by companies for surveillance capitalism. Therefore, the question is asked whether a commercial party can be responsible for the data processing or data collection of the smart campus of TU Delft. According to Valks, there is currently no commercial party involved (B. Valks, personal communication, March 9, 2020). However, he stated that it is not impossible that a commercial party may contribute to the development in the future. Thereby, he states the university will always handle, control the data, and process the data at TU Delft. There are no suggestions given for commercial parties, which makes it only an indication.

In the Smart Campus Delft, there is no general governance about which direction this campus should follow (B. Valks, personal communication, March 9, 2020). However, the direction of governance is important since you should not only take in mind what benefits of the smart campus tools are (Valks et al., 2016). Herewith, it is required to consider how the campus should be organized and how, for example, new sensors should be managed. Thereby, the risks need to be identified.

According to the GDPR (Autoriteit Persoonsgegevens, n.d.), being transparent about what data you want to collect and the purpose why you collect data is important. It must serve a genuine purpose. For example, monitoring the work of a single employee will not serve a genuine purpose.

However, monitoring the work of all employees might serve a genuine purpose since it may contribute to safety in the office or energy saving. Valks explains that if the users have been told why you use their data and how their data is processed, it makes the purpose more transparent and thereby explains why it is helpful for them (B. Valks, personal communication, March 9, 2020). Therefore, more people may want to contribute. To be more transparent, a big communication trajectory needs to be set up that takes a long time and must consist of a lot of repetitions. Communication could be done by big screens, by informing people, and by workshops.

4.1.4. The future smart campus

The next steps within smart campus tools on TU Delft will most probably focus on applications to show available study places without PCs (Valks et al., 2018). This shift is expected since the number of students that have laptops on campus is increasing and the number of desktop PCs is decreasing. Moreover, there is a shift from applications that show booking information to applications that show how many people there are in the room.

At present, the type of collected space use data at universities is always aimed at levels of frequency and occupancy and not at the identity or activity of the user. Furthermore, for most tools the space use information is measured by the booking system more than by real-time data. The most used sources for data collection are self-booking systems and login data from desktop PCs. Of course, the development of smart campus tools is still growing. Especially the accuracy of sensors is rapidly improving. Besides that, outputs from various sensors are combined to complement the results. Within science, attention is paid to how the output from sensors leads to a meaningful number, e.g. the number of persons in a room.

Valks explains that one of the significant challenges at TU Delft is how to embed the smart campus tools in the organization (B. Valks, personal communication, March 9, 2020). The constraints within the project are mostly organizational. Who should do what, who is responsible for what and what are the benefits? It is very hard to find examples of how this should be done. Moreover, the different stakeholders within the project are dependent on each other and they need to be aligned for efficient development. For education rooms, most persons how useful this could be because these rooms are too expensive to have it unused. For study spaces, everyone also recognizes the benefits. In offices the use of smart campus tools may be harder to explain. This is because within universities most employees have stationary workspaces, so they have no need to find a workplace. The tools are most useful for flexible spaces.

Valks expects that in the future, campus management on a smart campus will in some ways be reactive instead of predictive. Things happen suddenly and cannot be predicted by smart campus tools. He names an example of a professor that wins a grant and instantly needs a laboratory for research. However, in many ways, campus management could become more proactive with the help of the tools.

At this moment it is unlikely that there will be a centralized integrated smart campus that consists of involvement of third parties or commercial parties. In fact, the international and Dutch smart campuses are all in a preliminary state. However, as can be seen in this first part of the analysis, most universities surely want to become ‘smart’.

They are very eager to use new smart campus tools for the sake of a more efficient and more productive campus. Their ambitious approach is mainly focused on the development of a specific tool for a particular problem. At TU Delft, this is also the case. Specific smart tools are tested or are implemented while there is no governance to an integrated smart campus. In the coming years, more and more sensors are placed at TU Delft to improve real-time space use measurement in combination with the already present Wi-Fi measurements. To have collaborative users within the project, the campus focuses on transparency. The campus managers face many challenges, such as organizational challenges and therefore excessive time is required for further development.

4.2. Survey results

Now, the perception of users at TU Delft will be discussed and analysed, based on the survey results. As stated in the methodology section, the survey consists of two parts with a total of 38 questions. The distribution of the data about basic information as gender, type of degree and the faculty of the respondents is already discussed in the methodology chapter. Therefore, these will not be described here.

This chapter is structured along with the survey questions. The first section 4.2.1. describes the background information of the students, such as age and the year students started their study. The second section 4.2.2. focuses on the activities of the students on campus. The third section 4.2.3. discusses the students' perception of privacy in general. The fourth section 4.2.4. explains students' behaviour regarding privacy and their knowledge about it. Thereafter, the fifth section 4.2.5. analyses the current students' perception of privacy on campus. At last, the sixth section 4.2.6. analyses the desirability of the smart campus in the future and the perception of students towards the smart campus in regard to their privacy.

This part starts with descriptive statistics since there are many questions in the survey. Descriptive statistics are very useful to get a lot of numbers in a limited space. This survey has many questions and therefore the descriptive statistics can clarify and summarize the findings. If a question in this chapter is labelled as 'multiple-choice question', the students have the possibility to give multiple answers on the given options. The data is presented in concise tables. Besides that, descriptive statistics can help to easily find errors. Descriptive statistics are suitable for numerical variables only. Frequency tables are used for the presentation of the questions where respondents have chosen multiple answers.

4.2.1. Results: Student information

In this first section of the survey analysis, the background information of the students is presented. The distribution of the data will be explained in combination with the mean-value and the mode. Since this section is about background information, no correlation or tests will be used. The data will be presented in tables or graphs or both.

As can be seen from table 6, most of the respondents (35.8%) are aged between 18-20. No data is published about the total distribution of the student population of TU Delft. Therefore, these results cannot be compared to the student population and nothing could be concluded from the distribution in

the sample. However, the share is gradually decreasing as age becomes higher and only 11 respondents (7.4%) are 27 years or older. The average respondent in this survey is close to the middle label ‘’21-23”, according to the mean-value (μ = 3,05). This label is coded with value 3.

As already can be expected from the age of the respondents, most respondents (34.5%) started their study in 2019 while 13.5% started before 2016, as shown in table 7. However, not all people that started their study in 2019 are also new at TU Delft, as explained is section 3.8. Sample Representativeness.

Table 6

What is your age?		Frequency	%	Cumulative %
Valid	Under 18	0	0,0	0,0
	18 - 20	53	35,8	35,8
	21-23	46	31,1	66,9
	24-26	38	25,7	92,6
	27 years or older	11	7,4	100,0
	Total	148	100,0	

Table 7

What year did you start this study?		Frequency	%	Cumulative %
Valid	before 2016	20	13,5	13,5
	2016	12	8,1	21,6
	2017	26	17,6	39,2
	2018	39	26,4	65,5
	2019	51	34,5	100,0
	Total	148	100,0	

What can be concluded from showing the distribution of the background information of the respondents is that most of the data is distributed as can be expected at a university. In addition, it could be concluded that the population at a university is considerably homogeneous with respect to a population in a city. At a university, all students have the same level of education and approximately the same age.

4.2.2. Results: Student activities

The next multiple-choice question gives insight into the type of activities of students at TU Delft. The secondary analysis already demonstrated for which activities various universities are implementing smart tools. Table 8 and figure 4 show that most of the students attend lectures (93%) when they are on campus. Besides the lectures, the two activities where most smart campus tools are focused on, self-study and group work both score high. Apart from the core activities at the university, there are no major additional activities on campus at TU Delft given by the respondents.

Figure 4

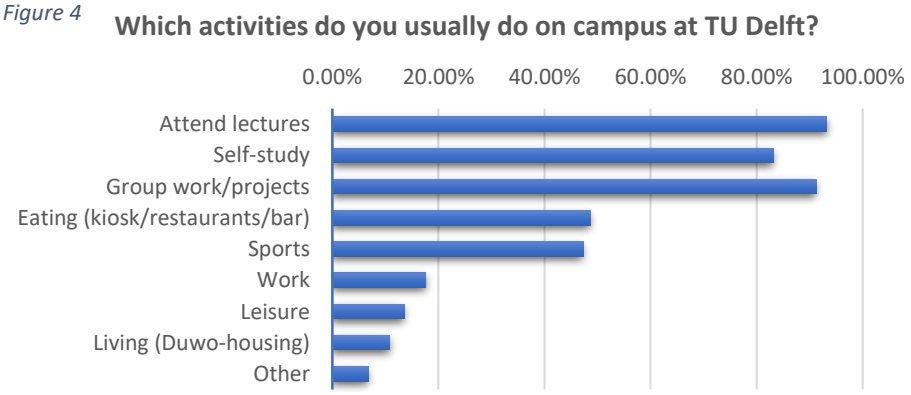

Table 8

Which activities do you usually do on campus at TU Delft?	Frequency	Mean
Attend lectures	138	,93
Self-study	123	,83
Group work	135	,91
Eating	72	,49
Sports	70	,47
Work	26	,18
Leisure	20	,14
Living	16	,11
Other	10	,07
Valid N (listwise)	148	

Table 9 and figure 5 show that the frequency that students are on campus at the TU Delft in a regular week, is in most cases 5 times a week (35.2%). Only 7.6% of the students are less than 3 times a week on campus at TU Delft in a regular week and 18.6% of the students are more than 5 times a week on campus. This number can only be used as an indication since the timetable of courses and visits to the campus vary per week.

Table 9

How often do you go to the campus at TU Delft in a regular week?		Frequency	%	Cumulative %
Valid	More than 5 times a week	27	18,6	18,6
	5 times a week	51	35,2	53,8
	4 times a week	28	19,3	73,1
	3 times a week	28	19,3	92,4
	2 times a week	5	3,4	95,9
	once a week	3	2,1	97,9
	Less than once a week	3	2,1	100,0
	Total	145	100,0	

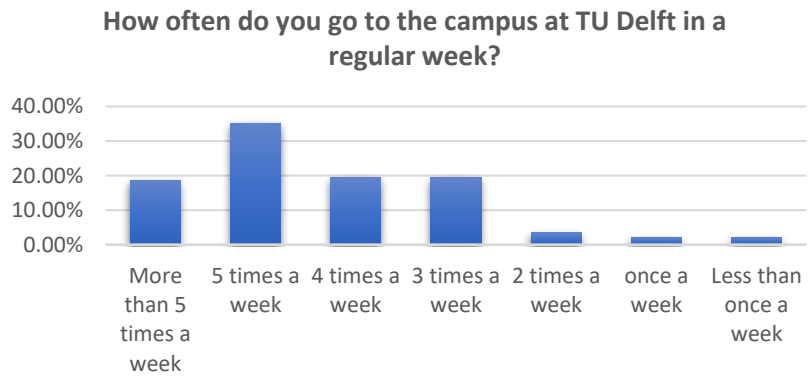

Figure 5

Table 10 and figure 6 present that every student that answered this multiple-choice question, claim to connect to the campus network with their mobile phone when they are on campus. Furthermore, 99% also connect to the network with their laptop. Approximately 40% of the students regularly make use of a desktop computer from the university. Other devices, as tablets and smartwatches are rarely mentioned.

Table 10

What devices that can be detected on campus do you use on campus at TU Delft?	N	Mean
Mobile phone	145	1,00
Laptop	144	,99
Tablet	10	,07
PC from university	55	,38
Smartwatch	9	,06
Other devices	1	,01
Valid N (listwise)	145	

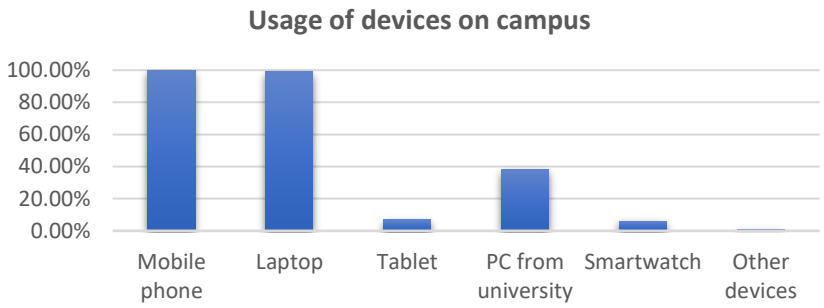

Figure 6

For the multiple-choice question (n-value = 119) about students' usage of smart tools, a comparison of means shows that the tools are not often used in general, see table 11 and figure 7. The most used tool is the tool to book a project room (52%). Almost a third (32%) of the students report that they do not use tools at all. As described in the secondary analysis, many smart tools are still in development or are being tested. This could explain the discrepancy between the existing smart campus tools at TU Delft and the actual use of it by students.

Table 11

For which of the following situations do you use tools on campus that are provided by the university?	Mean	Variance
To find an available PC workplace (desktop)	,16	,135
To find an available study space without a PC	,15	,129
To book a project room	,52	,252
To book a study place	,30	,213
Indoor navigation	,12	,105
I do not use tools for any of these situations	,32	,219

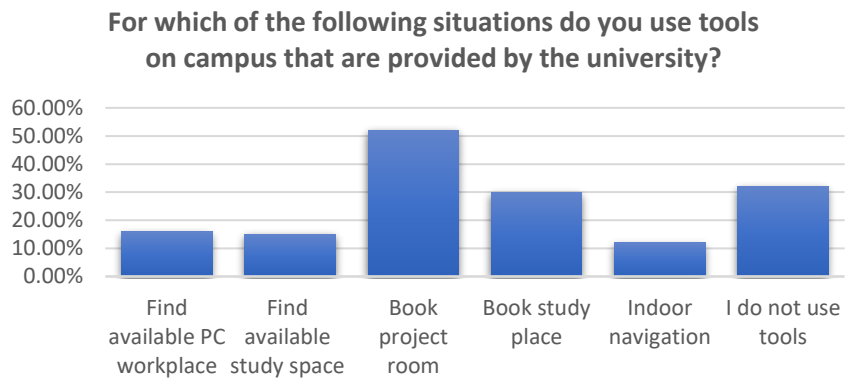

Figure 7

Overall, these questions show that the activities on campus are almost all linked to the core activities of a university while strategic documents of TU Delft indicate that the campus should become a small city with diverse activities and non-educationally related activities. However, this development cannot yet be deduced from these results.

4.3.3. Results: Perception of privacy in general

As can be seen in the following table 12 and figure 8, students are most concerned about their location information if it is used for real-time measurements by advertisers and commercial services ($\mu = 4.01$). The value 5 stands for 'very concerned' and the value 1 stands for 'very unconcerned', the value 3 is 'neutral'. Cronbach's Alpha in this question is 0.796 with n-value of 125 (**see table X-12 in Appendix A: factor and reliability analysis).** Besides the high mean value, the variance value is low which implies that the students are relatively unanimous in their concerns ($\sigma^2 = 0.90$). Students are the least concerned about their location information if it is used by the university ($\mu = 2.65$). Hence, students experience fewer concerns at a university than at a government, which is a relevant result. Thereby, at the government, the variance-value is the highest, which implies students find this debatable. The combination of the means of concerns is ($\mu = 3.30$). Overall, people are thus slightly concerned about their location information if this is used for real-time measurement by various organisations.

Table 12

How concerned are you about your location information if this is used for real-time measurements by the following organisations?	Mean	Variance
The government	3,10	1,158
The university	2,65	1,053
Advertisers/Commercial services (Google, OV9292, Facebook etc.)	4,01	,895
Commercial parties on campus (restaurants/bars/kiosk/shops)	3,46	1,169

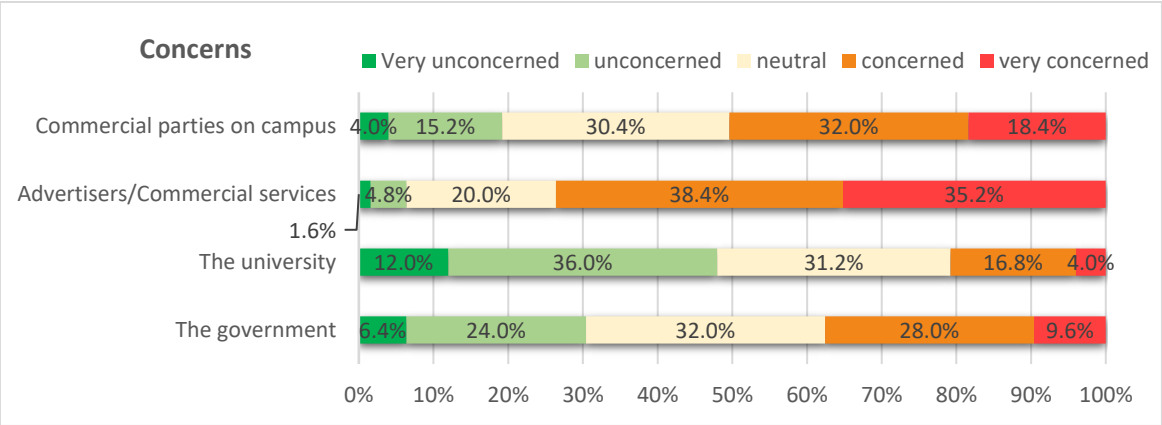

Figure 8

To answer the question which students from a particular faculty experience the highest concerns, the means of the computed variable of 'concerns' is compared in figure 9 (see Appendix A: factor and reliability analysis). Herein, the faculty is the independent variable. The faculty TBM (Technology, Policy and Management) is excluded since the number of missing values listwise was too high. This figure explains that students that belong to EWI (Electrical Engineering, Mathematics & Computer Science) have the highest concerns ($\mu = 3.63$). IO (Industrial Design Engineering) and 3ME (Mechanical, Maritime and Materials Engineering) are relatively unconcerned ($\mu = 2.98$).

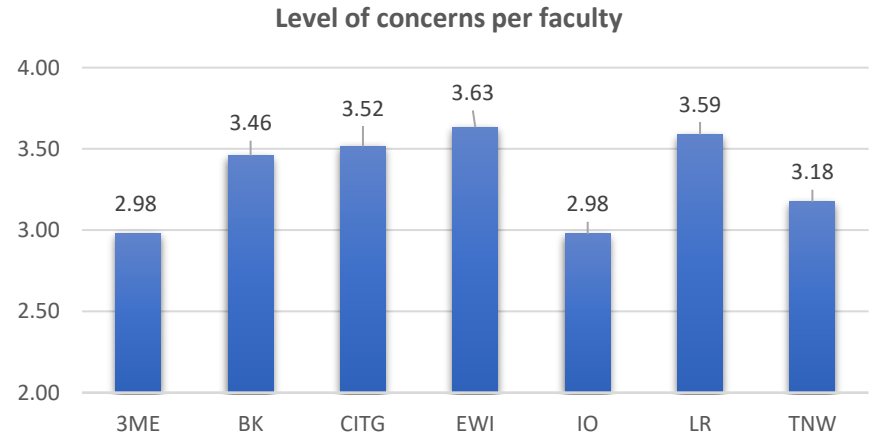

Figure 9

Table 13 and figure 10 show the results of the question about perception of ability to control personal information on campus. In this question the value 5 stands for "fully in control" and the value 1 stands for "fully out of control". Students perceive to have the most ability to control access to personal data that comes from offline behaviour on campus, such as conversations ($\mu = 3.11$ and n-value = 124). However, this type of data has the highest variance value and students are thus relatively divided in their perception ($\sigma^2 = 1.52$).

Students also perceive to have a strong ability to control access to data about their physical location on campus. Students perceive less ability when it comes to the control they have over access to data about their online behaviour ($\mu = 2.77$). These results indicate that students worry less about information that could be derived from offline behaviour over online behaviour.

Furthermore, there is a moderate negative relationship between the component 'concerns' and 'ability to control data of online behaviour' (Spearman's Rho = 0,241, p = 0.007). In short, if a student has more concerns, he also perceives to have a lower ability to control.

Table 13

How do you perceive the ability to control access to the following types of personal data?	Mean	Variance
Your physical location on campus	3,11	1,044
Your online behaviour on campus	2,77	1,210
Your usage of services on campus	2,92	1,075
Offline behaviour on campus (conversations)	3,55	1,518

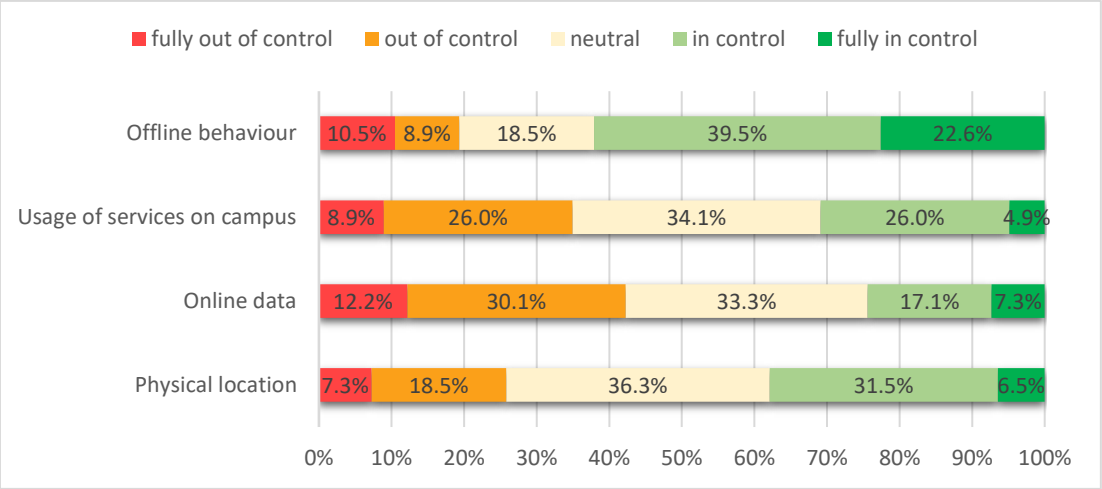

Figure 10

In short, these questions show that the researched variables in this thesis are not regarded as the most important variables by students. They have the least concerns when a university uses their location information for real-time measurements and in general, they have the perception that they have a strong ability to control data about their physical location on campus.

4.3.4. Results: Students' knowledge and behaviour of privacy on campus

Students are relatively most familiar with the content of the GDPR, although the mean value is in between the labels 'slightly familiar' and 'somewhat familiar'(μ = 2.53, n-value =125), see table 14 and figure 11. However, as can be derived from the variance value of the GDPR-scale, students differ strongly in how familiar they are with the GDPR. In this question, the value 5 is very familiar and the value 1 is not at all familiar. Privacy policies are relatively unknown (μ = 1,50).

Table 14

How familiar are you with the content of the following?	Mean	Variance
The General Data Protection Regulation or GDPR (AVG in Dutch)	2,53	2,058
The privacy statement of TU Delft	2,10	1,313
Privacy policies from other services on campus	1,50	,720

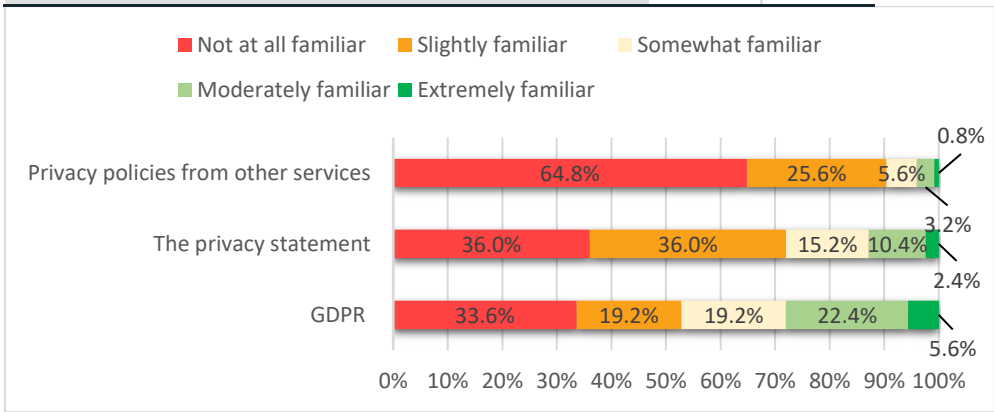

Figure 11

Table 15 shows that 33% of the respondents declare to be selective in sharing location information on campus, which is high compared to an American research of Boyles et al. (2012). In Boyles et al. (2012), only 19% of cell phone owners have turned off the location tracking feature on their cell phone. This dissimilarity could be caused by multiple factors, e.g. the year of the research, the awareness of the sample, formulation of the question or cultural aspects.
The other 67% of the respondents are not selective and do not do anything to protect their location information on campus. If this question is answered with “yes” the respondents are asked how they are selective. The most common answers are that students do not turn their GPS on at all or that students are selective with turning their GPS on. Furthermore, students do not always have their Wi-Fi or Bluetooth on. A few respondents state that they turn off location tracking in apps when this is optioned.

Table 15

	Frequency	Mean	Variance
Are you selective in sharing your location information on campus? (e.g. do you turn your GPS off?)	115	1,67	,223

In short, it could be stated from these two questions, that a major part of the students does not have a considerably high understanding of the GDPR, the TU Delft privacy statement and privacy policies on campus. In addition, relatively many students do take action to protect their location information on campus compared to the research of Boyles et al. (2012). Still, this is only a third of the students that take action to protect their location information.

4.3.5. Results: Analysis of privacy perception on campus

Almost every student (98%) thinks that via Wi-Fi, their presence can be detected on campus, see table 16 and figure 12 (n-value = 120). 'RFID', 'camera detection' and 'Bluetooth' are also often mentioned as methods. Infrared and wearable sensors are not seen as methods that disclose students' presence on campus. The method 'camera detection' has the highest variance value and there is thus the least consensus about this method. The outcome of this question can already be compared with the actual methods that are used to collect information at TU Delft. As the students already expected, their presence is indeed disclosed via the Wi-Fi network on campus. Infrared is also used at TU Delft. The other connection methods are not in use yet. However, this could be the case in the future. This was a multiple-choice question where multiple answers were possible.

Table 16

Via what of the following connection methods do you think you disclose your presence on campus?	Mean	Variance
Wi-Fi	,98	,025
Bluetooth	,38	,236
RFID	,69	,215
Camera detection	,49	,252
Infrared	,08	,070
Wearable sensors	,08	,070
Other	,02	,017

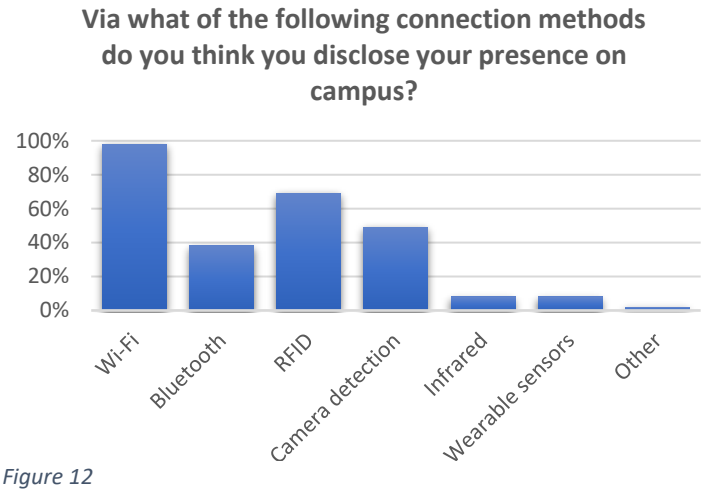

Figure 12

Table 17 and figure 13 present the results of the question: "Do you think you are sharing your location information with the university when you are on campus?", which 47.83% of the students answered with "probably yes". 6.96% is sure that they share location information and over 45% of the students do not consent that they share their location information with the University. This means that almost half of the student sample is not knowing for sure that they share location information with the university when they are on campus. The mean value of this question is (μ = 2.63), which implies that on average, the students are between 'might or might not' and 'probably yes'.

Table 17

Do you think you are sharing your location information with the university when you are on campus?		Frequency	%	Cumulative %
Valid	Definitely yes	8	7,0	7,0
	Probably yes	55	47,8	54,8
	Might or might not	30	26,1	80,9
	Probably not	16	13,9	94,8
	Definitely not	6	5,2	100,0
	Total	115	100,0	

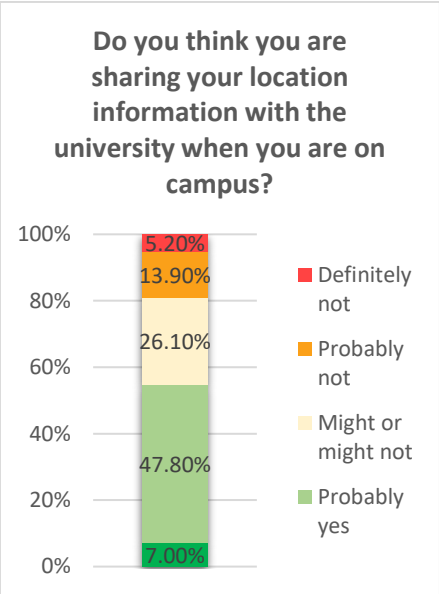

Figure 13

To the question: “Are you aware of what specific information you share on campus?”, over half of the students are unaware of what specific information they share on campus, see table 18 and figure 14 (54.4%, n-value 114). This question mainly focuses on the content of the information. Almost a quarter is very unaware (24.6%). Only 6.2% of the students are aware or very aware of what specific information they share on campus. The mean value of this question is (μ = 2,04), which is close to the label ‘unaware’ (2). This means that the majority of the students (93.9%) on campus are not aware of what specific information they share on campus.

Table 18

Are you aware of what specific information you share on campus?		Frequency	%	Cumulative %
Valid	Very unaware	28	24,6	24,6
	Unaware	62	54,4	78,9
	Neutral	17	14,9	93,9
	Aware	6	5,3	99,1
	Very aware	1	,9	100,0
	Total	114	100,0	
Total		153		

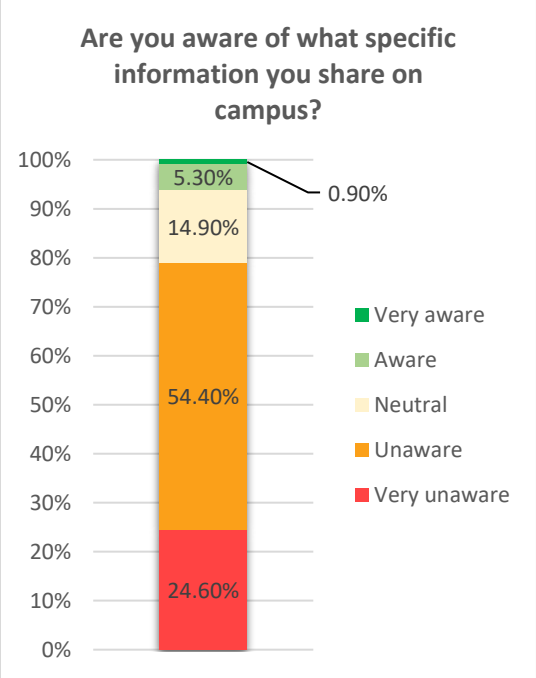

Figure 14

A part of the objectives was to find out whether students from a particular faculty have a different awareness of the data that they share on campus. In figure 15, the results of the awareness per faculty are shown. Again, the faculty is the independent variable and the faculty TBM is excluded. In this figure, the label 5 is 'very aware' and label 1 is 'very unaware'. The label 3 is 'neutral'. Students of EWI (Electrical Engineering, Mathematics & Computer Science) state that they have the highest awareness. Students of IO (Industrial Design Engineering) state that they have the lowest awareness.

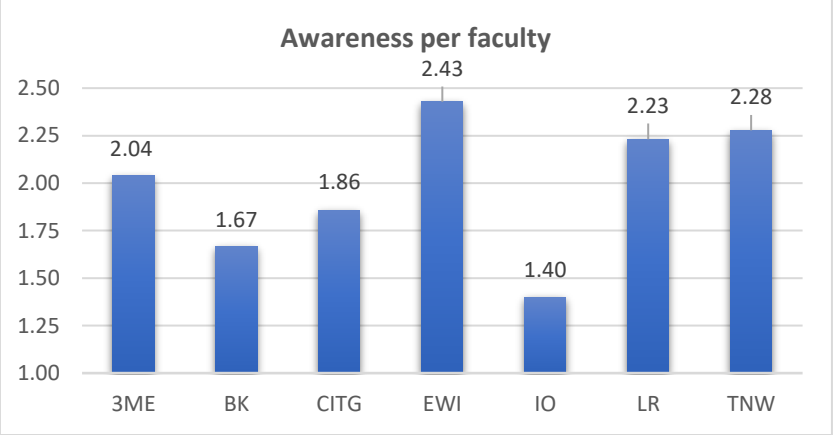

Figure 15

The next question focuses on the data handling of the university, see table 19 and figure 16. The number of respondents in this question is (n-value = 115), with a mean of (μ = 1,98), whereby the value 1 is 'nothing' and the value 4 is 'much'. Generally, the students state that they have very little understanding of what the university is doing with their data.

Over 75% do not feel to understand, or 'very little', what the university is doing with their data. 23.5% does understand some about how the university handles their data and no students claim to know much about what the university is doing with their data. Hence, a major part of the student population does not know what the university is doing with their data.

Table 19

How much do you feel you understand what the university is doing with your personal data?		Frequency	%	Cumulative %
Valid	Nothing	29	25,2	25,2
	Very little	59	51,3	76,5
	Some	27	23,5	100,0
	Much	0	0,0	100,0
	Total	115	100,0	

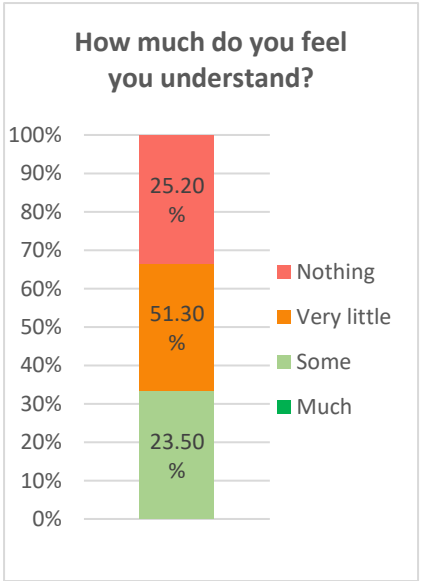

Figure 16

Roughly a third of the students (33.0%) describe their ability to control their location information that they share with the university when they are on campus as “fully out of control”, see table 20 and figure 17 (n-value = 115). 26.0% of the students claim to have the ability to slightly control or fully control their location information on campus. The mean value of this question is (μ =1,95), wherein the label 1 is ‘fully out of control’ and the label 4 is ‘fully out of control’. This mean value is close to the label ‘slightly out of control’. In short, almost three-quarters of the student population describe their ability to control as out of control or fully out of control.

Table 20

How would you describe your current ability to control (rectify/turn off) your location information that you share with the university when you are on campus?		Frequency	%	Cumulative %
Valid	Fully out of control	38	33,0	33,0
	Slightly out of control	47	40,9	73,9
	Slightly in control	28	24,3	98,3
	Fully in control	2	1,7	100,0
	Total	115	100,0	

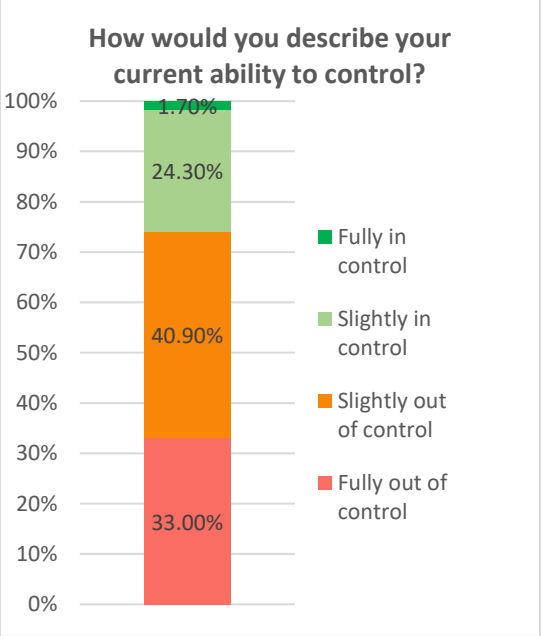

Figure 17

The students generally do not perceive the potential risk of losing information or misuse when they share information with the university when they are on campus, see table 21 and figure 18. Almost 60% perceives the potential risk to be moderately low or low. In this question the label stands for 'low risk' and the label 5 stands for 'high risk'. The mean-value (μ =2,38, n-value = 115) shows that the overall potential risk is 'moderate' to 'moderately low'. The percentage of students that perceive a moderately high risk or a high risk is 9.6%.

Table 21

How do you perceive your potential risk of losing information or misuse when you share information with the university when you are on campus?		Frequency	%	Cumulative %
Valid	Low risk	20	17,4	17,4
	Moderately low	46	40,0	57,4
	Moderate	38	33,0	90,4
	Moderately high	7	6,1	96,5
	High risk	4	3,5	100,0
	Total	115	100,0	

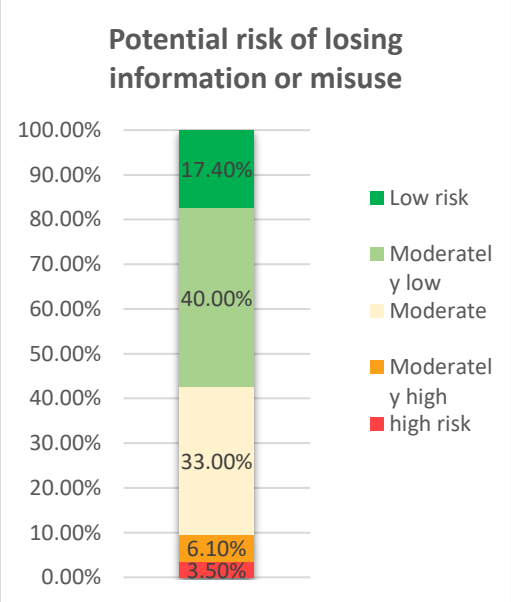

Figure 18

Table 22 and figure 19 show that the number of students that describes their perception of protection of personal data on campus as "unsafe" or "very unsafe" is very small (8.8%). The n-value is 114 in this question. The labels are 'very safe' for 1 and 'very unsafe' for 5 (μ = 2,64). Most of the students describe their perception as "neither safe nor unsafe". Almost 45% of the students feel "safe" or "very safe". There cannot be stated that a major part of the students perceives to be safe. However, a major part of the students perceives not to be unsafe or very unsafe about the protection of their personal data on campus.

Table 22

In level of safeness, how would you describe your current perception of the protection of personal data on campus?		Frequency	%	Cumulative %
Valid	Very unsafe	3	2,6	2,6
	Unsafe	7	6,1	8,8
	Neither safe nor unsafe	54	47,4	56,1
	Safe	46	40,4	96,5
	Very Safe	4	3,5	100,0
	Total	114	100,0	

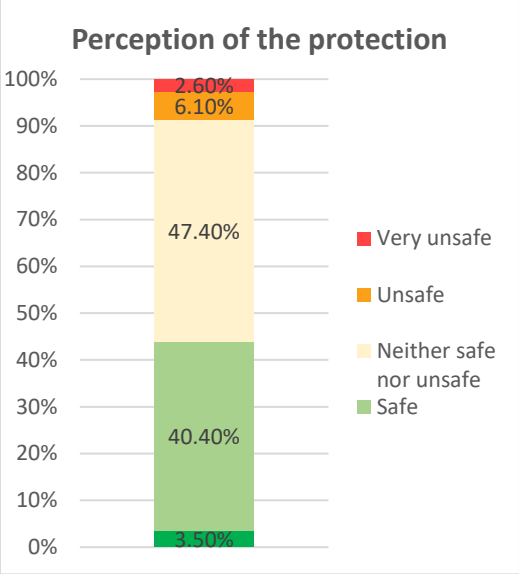

Figure 19

In short, this section gives some interesting insights into students' privacy perceptions on campus. Most students are not aware that they share information with the university, they are not aware of the content of the information and they do not know how the university processes their data. Furthermore, they do not perceive to have the ability to control their data when they are on campus. Meanwhile, the students perceive no potential risks of loss or misuse of information and they do not feel unsafe about their personal data. These results could indicate that students do not perceive any risks because they are unaware of the fact that personal data is collected about them.

Another result from this section is the distribution of awareness among students from different faculties. Students of EWI (Electrical Engineering, Mathematics & Computer Science) state that they have the highest awareness and students of IO (Industrial Design Engineering) state that they have the lowest awareness.

4.3.6. Results: Privacy on future smart campus

The next 6 questions are presented in the concise table 23 (n-value = 106). These questions have an equal Likert-scale design and therefore these questions are combined. The Likert-scale consists of the following labels:

1. Very uncomfortable
2. Uncomfortable
3. Neutral
4. Comfortable
5. Very comfortable

In this question a value of 1 stand for “Very uncomfortable” and a value 5 stand for “Very comfortable”. The component ‘comfortability of being tracked’ is a combination of the mean values of all those questions ($\mu = 2.48$) and is labelled as ‘uncomfortable’. Furthermore, this ‘comfortability of being tracked’ component has a moderate positive relationship with the component ‘ability to control data of online behaviour’ (Spearman’s Rho = 0.363 p = 0.00). This indicates that if a student’s ability to control data of online behaviour is higher, his comfortability is being tracked is also higher.

As can be derived from table 23, students are most comfortable if their personal data is used for study services such as printing or finding available workplaces ($\mu = 3.49$). The students are also relatively comfortable when their personal data is used for research or for the sake of their ($\mu = 3.34, 3.33$). The students are most opposed if their personal data is used to sell it to third parties ($\mu = 1.21$). Besides third parties, students are also opposed if their personal data is used for targeted advertisements or if it is just stored ($\mu = 1.21, 1.81$). Students are most divided if their personal data is used for measurements for their study progress, as can be assumed from the variance-value ($\sigma^2 = 1.379$). Briefly, students are more comfortable if their personal data is used for study services and educational purposes than for commercial purposes.

Table 23

How comfortable would you be if your personal data on campus is used, without specifically stated for what purpose this is used, for the following?	Mean	Variance
For measuring your study progress (e.g. presence)	2,57	1,379
To navigate (e.g. to lecture room, to bus stop)	3,33	1,335
For study services (printing, finding available workplaces)	3,49	1,045
For targeted advertisements	1,54	,590
For offering personal services (e.g. psychological consult, finding a workplace)	2,55	1,287
For research	3,34	1,169
To sell it to third parties	1,21	,321
For being stored	1,82	,808
Valid N (listwise)	107	

Besides the comfortability to the usage of personal data, the students are also questioned what types of information they find acceptable or unacceptable if this is tracked on a smart campus. In this table, the mean value 1 represents “unacceptable” and 3 represents “acceptable”. As presented in table 24, students find study participation the most accepted purpose for being tracked (μ = 1.86). Furthermore, students find it acceptable if their location is tracked on a smart campus (μ = 1.80). Tracking offline behaviour on campus is definitely not accepted among the students (μ = 1.03).

The factor analysis (See Appendix A: factor and reliability analysis) resulted in one reliable component of acceptability, named: ‘acceptability of data-use of online information on campus’. This component has a moderate positive relationship with the component ‘comfortability’ (Spearman’s Rho = 0.248, p = 0.01). Hence, a higher ‘acceptability of data-use of online information on campus’ comes with a higher ‘comfortability’, to a certain extent.

Table 24

What of the following would you find acceptable if this is tracked on a campus?	Mean	Variance
Your study participation (e.g. presence in lectures)	1,86	0,782
Your location	1,80	0,688
Your activities (e.g. study, sport, leisure)	1,69	0,855
Your emotional well-being (e.g. e-consult, psychologist)	1,44	0,551
Your biometric information	1,29	0,630
Your transactions	1,39	0,683
Your online behaviour	1,27	0,576
Your offline behaviour	1,03	0,166
Valid N (listwise)	107	

Table 25 and figure 20 show that most of the students (59.8%) find it unacceptable if their location information is used for commercial purposes on campus. Only 5.5% finds this acceptable. The mean-value is also very low (μ = 1.62), with 1 as ‘unacceptable’ and 5 as ‘acceptable’. Students do clearly not see any space for commercial purposes that use their location information on campus.

Table 25

What would you think if your location information on campus would also be used for commercial purposes such as food consumption and advertisements?		Frequency	%	Cumulative %
Valid	Unacceptable	64	59,8	59,8
	Slightly unacceptable	28	26,2	86,0
	Neutral	8	7,5	93,5
	Slightly acceptable	6	5,6	99,1
	Acceptable	1	,9	100,0
	Total	107	100,0	

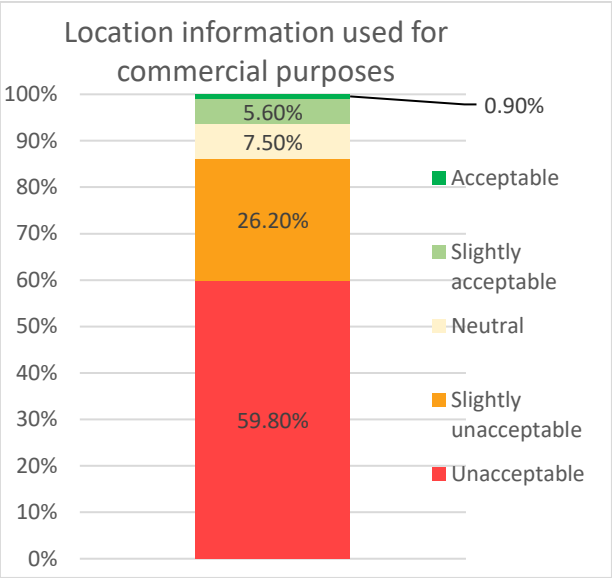

Figure 20

The next 5 questions are presented in a concise table. These questions have an equal Likert-scale design and therefore these questions are combined. The Likert-scale starts with value 1 that represents "definitely not" and ends with value 5 "definitely yes". The first two questions have an n-value of 107 and the 3 last questions have an n-value of 106.

As shown in table 26, **s**tudents are most willing ($\mu = 3.05$) to disclose their presence via cameras to improve education. Thereafter, students are most willing to disclose their location information via Wi-Fi tracking if this helps the efficiency of space use ($\mu = 2.92$).

Students are the least willing to use an app such as Quantified Student wherein biometric data is used to improve the learning experience ($\mu = 2.07$). Therewith, students are not willing to use tools at all If a commercial party would take care of it (($\mu = 2.02$). The resistance to involvement of commercial parties is hereby again acknowledged.

Important to notice here is that two questions have ambiguous formatting; therefore, these questions could not be answered with certainty. An assumption is made that students that answered "yes" or "definitely yes" at the second question, are willing to disclose their presence in lecture rooms via cameras if this is used for improvements of education. Another assumption is made in the third question. Hereby, it is assumed that students that answered "yes" or "definitely yes" are willing to disclose their presence via sensors if it becomes easier to find a free desk.

Table 26

	Mean	Variance
Would you still use these tools if not the university but a commercial would take care of the smart campus?	2,02	1,056
Currently, on some Dutch universities, cameras are used to monitor students' occupancy in lecture rooms. Would you mind to disclose your presence if this is used for the purpose of improving education?	3,05	1,309
Another tool is a sensor under a desk at a working space that detects if the desk is occupied. Do you mind that your presence can be detected by these sensors if it becomes easier to find a free desk?	2,65	1,982
Wi-Fi tracking is also used within Dutch universities to monitor movements of people on campus and to find out what places are often used and what places are less used. Would you disclose your personal information if your data is used for efficient use of the campus?	2,92	1,982
Quantified Student is an application in development that aims to create a better learning experience for students. For this application, biometric information will be tracked, such as hours of sleep and level of stress. Besides that, other data as time on campus, alcohol consumption and study time is also tracked. If this application would be available for you in exchange for your information, would you use it?	2,07	1,148

Most students (53.8%) do “somewhat agree” or do “strongly agree” to the statement “I am willing to disclose my location information if this helps the functioning of space on campus.”, see table 27 and figure 21**.** 25.5% of the students disagree with this statement. The mean value μ = 3.29, which is between the label 3 ‘neither agree nor disagree’ and ‘somewhat agree’. Almost three-quarters of the students are thus not against the disclosure of their location information if this is used for the purpose of functioning of space.

Table 27

I am willing to disclose my location information if this helps the functioning of space on campus.		Frequency	%	Cumulative %
Valid	Strongly disagree	8	7,5	7,5
	Somewhat disagree	19	17,9	25,5
	Neither agree nor disagree	22	20,8	46,2
	Somewhat agree	48	45,3	91,5
	Strongly agree	9	8,5	100,0
	Total	106	100,0	

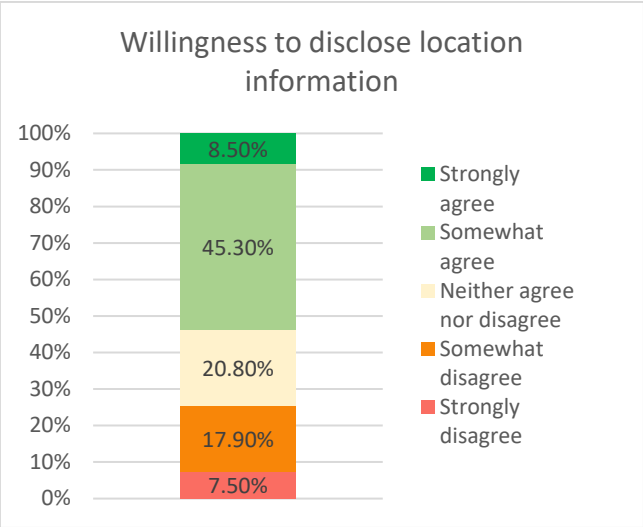

Figure 21

The results in this section partly overlap. Therefore, the outcomes that point in the same direction strengthen each other. These results provide an indication that the purpose of the data collection is very important for students as well as the involved party. Data collection for educational purposes are seen as worthwhile and therefore, students are willing to share more data such as location information for efficiency of space use. Moreover, according to section 4.3.3. 'Results: Perception of privacy in general', the university is perceived as a trusted party that will not bring many risks with it while this section shows there is much resistance to the potential involvement of commercial parties with commercial purposes.

4.3.7. Results: Desirability of smart campus

In this section, the results of the questions about students' behaviour in the future regarding their privacy on campus and their desirability of the smart campus are presented. It is assumed that through participation in this time-consuming survey students are informed about a smart campus and that this questionnaire should set students thinking. From the results of this section, it is derived what the students' privacy perception is regarding their personal data on a smart campus of the future. Besides the quantitative analyses of questions, two open questions are also and the results are presented as well in this section, albeit in a qualitative way.

Table 28 and figure 22 **s**how that 15.1% of the students expect to see their effort to protect their location information on a smart campus in five years to be "much higher" in relation to their current effort. In total, 55.7% of the students expect to see their effort rise. Only 8.5% expects their effort to decrease and 0.0% expects to have much lower effort. These results imply that, in a time span of 5 years, students expect to see an increase in their effort to protect their location information on campus. This is validated by the mean value of $\mu = 3{,}11$ on a scale of 1 to 7, whereby value 1 stand for an increase of effort and value 7 stand for a decrease of effort. Hence, this mean value is closest to the label 'slightly higher'.

Table 28

How do you see your effort of protecting your location information on a (smart) campus in five years, in comparison to your current effort?		Frequency	%	Cumulative %
Valid	Much higher	16	15,1	15,1
	Moderately higher	14	13,2	28,3
	Slightly higher	29	27,4	55,7
	About the same	38	35,8	91,5
	Slightly lower	7	6,6	98,1
	Moderately lower	2	1,9	100,0
	Much lower	0	0,0	100,0
	Total	106	100,0	

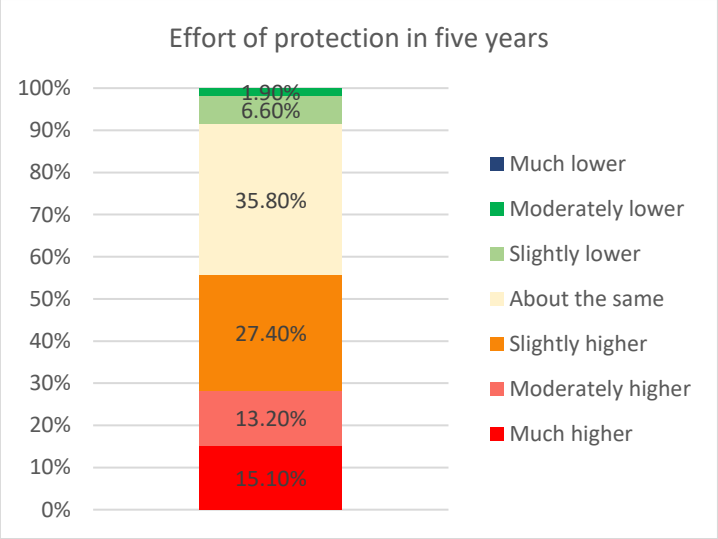

Figure 22

After the students indicated whether they expect their effort to increase or not, they were redirected to an open question where they could describe the reason why they expect their effort to increase or not. To provide an insight in the opinions of the students, a few interesting answers are quoted here. At first, the answers for an increase of effort are discussed and thereafter, the answers for a decrease or neutral effort are discussed. As shown in table 28, 59 students answered that they expect their effort to increase and 47 students expected their effort not to increase. From these answers, the following results come forward.

More effort

What definitively can be found in the answers of the students is that the survey set them to think and that some were not aware or were careless about sharing their information. On the other side, there are many students that describe that the technology is getting more advanced and that they find it hard to protect their data. Some students observe a movement towards more data-aware people. Furthermore, there is a consensus that as technology grows, methods improve and more and more data and location data is wanted, while privacy and transparency do not change with them.

Quotes:

"Because I do not appreciate being watched. I think campus efficiency is student's responsibility and I don't want a "Big Brother" situation. I would probably stop using electronic devices or attending lectures at all."
"Because when a university that is not as competent as they should be with technology tries to improve their technology, this just invites for bad practices."
"Because consensus raises about the power gained by gaining data and how it can be abused, which most likely will increase amount of user-friendliness and privacy friendly software."
"Due to the increasing awareness of side effects of big data."
"I am a digital rights and anonymity advocate (I work in cybersec and decentralization initiatives) and I have no interest in allowing anybody or anything track me or what I do in my life. I know this is going to get much more difficult, so I will need to step up my game in protecting my identity, including wearing forms of disguises to prevent facial recognition technology from identifying myself. The ONLY way I would mind sharing my data (location being the only thing I want to share) is if it is fully anonymized (which by the way is very easy to reverse, even with strong encryption standards) is to tell me which study spaces are more/less occupied. Otherwise everyone can fuck off with their bullshit "smart services.""
"I am not jet concerned about privacy, this makes me think that I underestimate the dangers probably and will most likely realize this more and more in the future. This due to the movement I am beginning to see towards more control and ownership over digitally tracked information."
"I assume technologies to grow faster than privacy"
"Personal info is getting a desirable and profitable good, it's already getting bought and sold"
"Well, if any of the priory mentioned things become reality, I definitely do not want to participate in them!"
"Your behaviour gets increasingly more monitored with the advance of the digital age, I think we should foster or privacy."

Less effort or the same

The answers why students expect to have less effort or the same effort to protect their location information are less extensively described than the previous question. Many students argue that the effort is really dependent on the way their location data is used. E.g. commercial or not.

Moreover, many students answered that they do not find their location information important, they do not care, are not concerned, do not see a reason to protect it, do not have time for it or they have lack of knowledge to protect it. A few answers also state that the technology is inevitably integrated with society and this cannot be stopped anymore. Noteworthy, there are relatively many students, in comparison to the previous question, simply do not know the answer to the question.

Quotes:

"Because it is inevitable in the world we live in to be in full control of our information."
"Because it is mostly used for good causes (e.g. study places)"
"I believe that technology is deeply integrated in our modern society and it will continue to develop. In 5 years time we'll be more used to having to accept giving up our privacy for the 'common good'. Nowadays we can't even visit a site without accepting cookies. I wouldn't be surprised if giving up our location information will become more and more normal."
"I feel I'm being monitored already, but I also trust that this data is not used in a negative way."

"I just think that it is beneficial for me personally to have this information shared. As I don't mind giving my information if it helps improve something like campus, that is of course if I can cancel it whenever I want, which is the idea I got from the questions."
"There's no fighting it. Technology will advance, people will always be weary of change in the beginning."

After filling in the survey, a large majority of the students (81.9%) does not find the smart campus desirable regarding the protection of their personal information, see table 29 and figure 23. 34.3% of the students think of a smart campus as undesirable and 20.0% think of a smart campus as very undesirable. This result implies that according to the students, they do not desire the idea of the TU Delft as a smart campus where everything is real-time tracked in regard to the protection of their personal information. This is acknowledged by the mean-value μ = 2,46, where 1 is the label 'very undesirable' and 5 is 'very desirable'. Hence, the mean-value is closest to the label 'undesirable'.

Table 29

What would you think of the TU Delft as a full 'smart campus' where everything is real-time tracked in regard to the protection of your personal information?		Frequency	%	Cumulative %
Valid	Very undesirable	21	20,0	20,0
	Undesirable	36	34,3	54,3
	Neither desirable nor undesirable	29	27,6	81,9
	Desirable	17	16,2	98,1
	Very desirable	2	1,9	100,0
	Total	105	100,0	

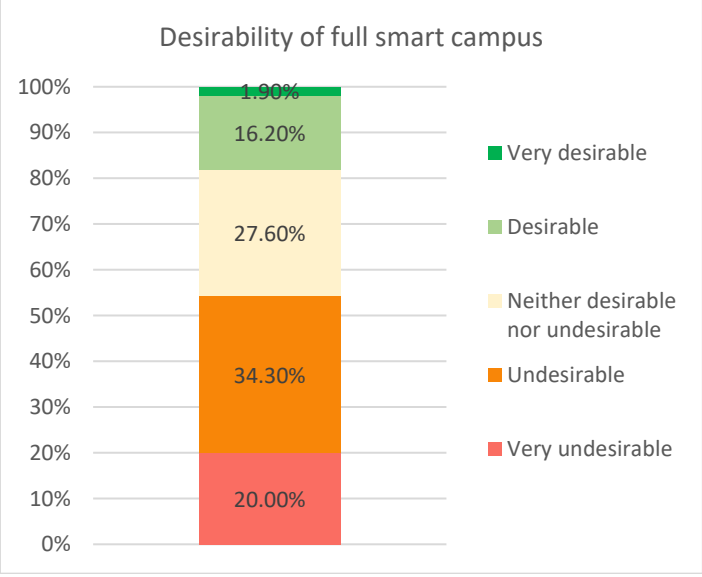

Figure 23

Table 30 and figure 24 show that 21.0% of the students perceive to be fully out of control of abilities to control personal data on a smart campus in five years. Besides, 43.8% would describe the ability to control their personal data on a smart campus in five years as 'slightly out of control'. Only 5.7% perceives the ability to be fully in control. Altogether, a mean value of μ = 2.02 shows that students describe their perception of ability to control their personal data as 'out of control' on a smart campus in five years. The mean value is close to 2, which is the label for 'slightly out of control'.

Table 30

How would you perceive the ability to control your personal data on a smart campus in five years?		Frequency	%	Cumulative %
Valid	Fully out of control	22	21,0	21,0
	Slightly out of control	46	43,8	64,8
	Slightly in control	31	29,5	94,3
	Fully in control	6	5,7	100,0
	Total	105	100,0	

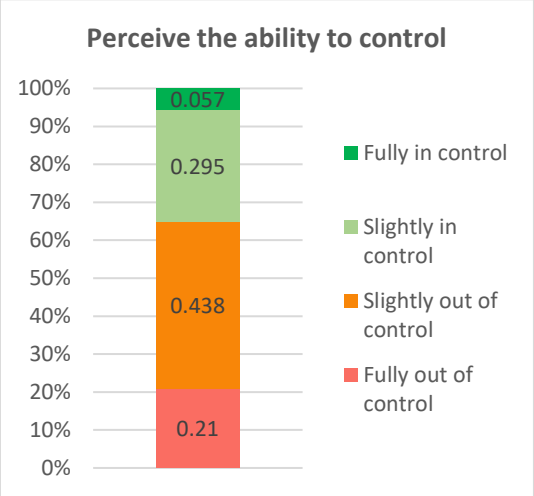

Figure 24

As described in the theoretical framework, people are willing to share personal information if there are expected benefits. Therefore, this question examines if students expect to benefit from sharing their data on a smart campus. In general, students are nuanced if it regards their expectations to benefit from the personal information that they share, see table 31 and figure 25. 6.7% of the students expect no benefits and 5.8% expect a great deal of benefits. 44.2% of the students expect very little benefits and 43.3% of the students expect some benefits in exchange for their personal information. Overall, the mean value is in the middle of the labels 'some' (3) and 'very little' (2) (μ = 2.48).

Table 31

How much do you expect to benefit from the personal information that you share on a smart campus?		Frequency	%	Cumulative %
Valid	None	7	6,7	6,7
	Very little	46	44,2	51,0
	Some	45	43,3	94,2
	A great deal	6	5,8	100,0
	Total	104	100,0	

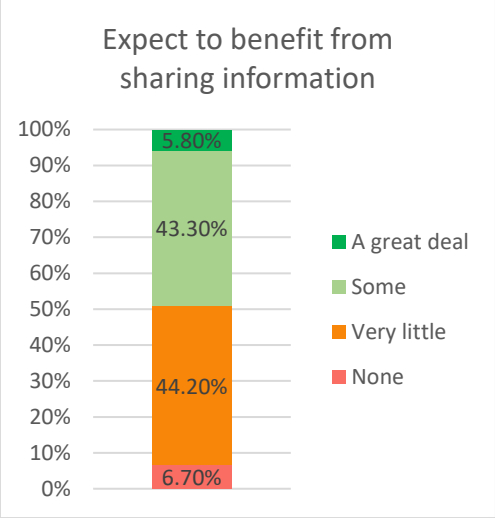

Figure 25

Table 32 and figure 26 show that the students are divided in their opinion about what the most essential safeguard is for user's personal information on a smart campus. 37.3% think that user awareness of protecting personal information is most essential. A third of the students think that government laws are the best safeguard. Less than 30% think that the responsibility is for the smart campus itself. Therefore, it is difficult to state what users think what the best safeguard is.

Table 32

In your opinion, what is most essential to safeguard user's personal information on a smart campus?		Frequency	%	Cumulative %
Valid	Users awareness of protecting personal information	38	37,3	37,3
	Laws from the government	34	33,3	70,6
	Measures taken by the smart campus itself	30	29,4	100,0
	Total	102	100,0	

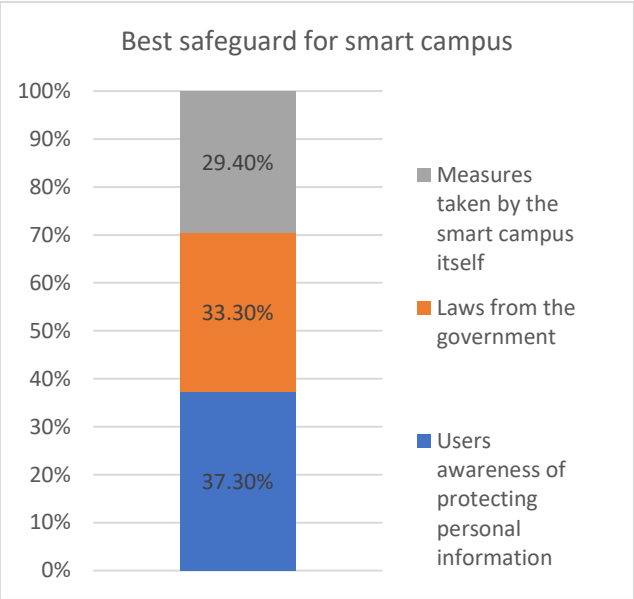

Figure 26

The questions in this section show that, in contrast to the campus management that strives to make their campus smart, students find it in fact not desirable in regard to protection of their personal information. Nevertheless, the previous section 4.3.6 concluded that students are willing to use smart tools if they serve an educational purpose and if their collection of their data is transparent.

5. Conclusion

Nowadays, the label smart is a very popular term in both research and society. Almost every service or product strives to become smart and personalized. This certainly also applies to the urban environment. Many cities strive to become smart for the sake of efficiency and sustainability. However, smart cities are often described from a technological and/or commercial perspective which results in a lack of attention for the effects of the smart city implementation on the ground level and for effects on society. At this point, these effects are not accurately described and the smart city seems to be a fuzzy concept. The concept smart city turns out to be a collective term for various technologies that focus on achieving goals with an emphasis on urban growth such as sustainability, social efficiency and political efficiency (Albino, Berardi, & Dangelico, 2015).

To do research on the effects on the users of the smart city implementation, a smart campus is used as a test case. In this test case, the user perspective on the ground level is examined. A campus represents a cross-section of the urban fabric on a small scale. On campuses, a similar development is going on as in smart cities. Smart campuses strive to become smart to make more efficient use of space and to make the life of the students easier. This research used the smart campus as a test case for the smart city because the smart campus is considered as a less complex phenomenon. The assumption, therefore, is that a smart campus is easier to implement than a smart city.

In this thesis, various sources and research methods are combined to provide insight in the perception of users on a smart campus regarding their personal data. This insight should recommend how smart campuses and smart cities should be designed in terms of users, data and privacy. The main research question in this thesis was: "*What can be learnt from the students' perception of location data on campus in comparison to the actual state at TU Delft, for the design of future smart campuses and smart cities?"*

To answer this research question, 5 objectives are formulated:

I. Explore how geographical data from students is used on international campuses, Dutch campuses and on the campus of TU Delft in particular.

II. Understand what the perception of students is on campus at TU Delft, regarding the geographical data that is collected about them.

III. Analyse which smart campus tools that collect and process geographical data from students are used at the campus of TU Delft.

IV. Evaluate if the perception changes when students are informed of the geographical data processed by smart campus tools and if there is a discrepancy between the actual state of the smart campus and the perception.

V. Make recommendations for the design of a user-empowered smart campus and smart city policy.

5.1. Answering the research question

To answer the research question, the five objectives are divided in three parts. The first part of this section focuses on the conclusion of actual state of location data-privacy on campus, which concerns objective I and III. The second part concludes what the students' perception of location data on campus at TU Delft is and if there is a discrepancy, which concern objective II and IV. Chapter 6 'Lessons for the smart city' concerns objective V and concludes what can be learnt from the discrepancy of these conclusions for the design of future smart campuses and smart cities.

5.1.1. Actual state of the smart campus at TU Delft

The phase of the smart campus TU Delft is preliminary. It consists of various pilots and tests of techniques. In general, this also applies to other Dutch universities and international universities. The smart campus as an integrated system that monitors everything on the campus is thus a long way off. The smart campus label is thus not applicable on the actual state of the university campus. However, the research definitely shows that there is a desire of universities to implement 'smart' in campuses to make more efficient use of space and to make the life of students easier.

Wi-Fi tracking is the most used type of data collection at TU Delft, while other types of data collection and sensors are rapidly improving. Via Wi-Fi, the location of the device is constantly tracked and, in some cases, coupled to the identity of the user. The smart campus tools are often aimed at measurements of occupancy and frequency of users within a room. On some university campuses, identity or activity is also measured. However, in Delft this is not the case yet. Nevertheless, the conclusion can be made that smart campuses are rapidly growing. This is a top-down driven process and users are barely involved, which makes research on users' perspectives very important. Furthermore, it is very important to bring this discussion, about how such a smart campus should function and the user's role in it, to the users itself.

5.1.2. Students' perception and discrepancy

It is assumed that a wide variety of variables contributes to the perception of students on campus regarding their personal data. These conclusions of these variables are drawn here and together provide insight into this all-embracing perception. As described in the previous section, the smart campus tools are used on a small scale on campus at TU Delft. Therefore, it is not surprising that from the survey indicates that the smart tools are not yet often used by the students.

The students are relatively unconcerned when an organisation as the university uses their location information for real-time measurements. Furthermore, students mainly have the perception that they have a strong ability to control data about their physical location on campus and students do not take action to protect their location information on campus. These conditions are thus important advantages for a university if they want to further develop the concept 'smart' into the campus since it is assumed that the collection of users' data, either actively or passively, is crucial for the systems to function.

Furthermore, most students are not aware that they share information with the university at all, they are also not aware of the content of the information and besides, they do not know how the university processes their data. Moreover, they do not perceive to have the ability to control their personal data when they are on campus. Hence, this research has shown that the perception of students regarding usage of their geographical data on campus at TU Delft, does not correspond to the data that is used and collected by TU Delft.

In contrast to these results, the students generally do not perceive a potential risk of losing information or misuse of the information that they share and they do not feel unsafe about the protection of their personal data on campus. The survey shows that most students trust that data is used by the university for genuine purposes and that the university will not make misuse of it.

These conclusions thus imply that in general, the awareness of the students is low and that the concerns about their protection of personal data on campus is also low. It could be stated that the control over the data collection is in the hands of the university, which seems to be a precarious situation for the students on campus regarding their personal data. Although the current situation is possibly not that precarious now, the university has the abilities to develop the smart campus independently.

These results also indicate that the purpose of the data collection is very important for students as well as the involved party. Data collection for educational purposes is seen as worthwhile and functional. Therefore, students are willing to share more data, such as location information for efficiency of space use or the disclosure of their presence in a lecture room for occupancy measurements. The survey shows that students perceive the university as a relatively trusted party that will not bring many risks of loss or misuse of shared data with it, in comparison to commercial parties. Meanwhile, there is much resistance to the potential involvement of commercial parties with commercial purposes. The secondary analysis demonstrates that a commercial party is not yet involved in the development of the smart campus. However, the involvement of commercial parties is not excluded in the future. No policies are found which exclude the involvement of commercial parties while strong governance is also absent.

Another result from this section is the difference in privacy concerns and awareness of students per faculty. The outcomes show that students from EWI (Electrical Engineering, Mathematics & Computer Science) have the highest privacy concerns and the highest privacy awareness while students from IO (Industrial Design Engineering) have the lowest privacy concerns and the lowest privacy awareness. The survey shows no clear indication for the difference in these results. Therefore, further research is needed.

The outcomes of the survey suggest that location data is relatively accepted if this is tracked on campus, in comparison to other data such as biometric information or data of online behaviour. Students expect to see an increase in their effort to protect this location information on campus in the coming years. Furthermore, the survey implies that, if it is up to the students, the smart campus is in fact not desirable in regard to protection of their personal information.

The perception of location data of students on campus at TU Delft varies per case and per purpose. In general, many students are not aware of the fact that they are being tracked by methods as Wi-Fi, cameras and infrared. They believe that their data is safe and used for the right purposes. It could be argued that with the current situation, the students have low awareness and low concerns but the extent to which they are tracked on campus is also relatively low. Although students perceive to know that their devices can be tracked via Wi-Fi, they are generally not aware of what data they share or how they can control this. This survey indicates that there is a discrepancy to a certain degree between what the students think they share with the university and what is actually collected and used by the university. This discrepancy is fixed and is likely to change in the future if the campus moves more towards a smart campus where more data is collected for more purposes. This may cause a decrease in transparency and a growing gap between the perception of data on campus and the actual situation.

6. Lessons for the smart city

The main difference of a smart campus compared to a smart city is that the smart campus seems to have more possibilities for their development, because the users relatively have high confidence and trust in the university as an organization. This trust can facilitate further integration of the smart campus. Furthermore, the purposes of a university are clear for the users and therefore the users are more likely to share data. The survey already implied that confidence in a government or commercial organisation as a data processor is lower than in a university. Within the smart city, purposes are probably less clear for the citizens. Therefore, it is expected that smart cities will experience difficulties in collaboration with their users. A solution for these difficulties is to have high transparency towards the citizens about which data is collected and for what purposes the data is collected.

The activities of the students on campus are almost all linked to the core activities of a university. The campus of Delft is not yet a small city with diverse activities and non-educationally related activities such as leisure. The survey showed that students have specific purposes to visit the campus, which are mostly educational and that are not constantly on campus. In the smart city as described in the introduction and theoretical framework, this is quite different. In these cities, the purposes vary widely and these purposes are far less unified and transparent.

The survey illustrates that many students do not have knowledge about what data Is collected, how data is processed or where data is stored. To find this out, they can visit the website to read the privacy statement. Compared to an average city, the students are far more educated on campus than the average citizen. It is expected that the average citizen will have less knowledge than these high-educated students. Therefore, the lack of knowledge about collected data, processed data and stored data possibly complicates the citizen's ability to protect personal data in a smart city.

This research implies that the smart campus is indeed a miniature version of a smart city. Hence, the smart campus is a suitable location to test implementation of smart technologies since the university is the owner of all the real estate. Besides that, much can be learned about the implementation of 'smart' in an organization.

In the city itself, this will be more complicated, although the smart campus gives some substantial insights. A major difference between a smart campus and the smart city is the user. On a campus, the population is well-educated and they are more informed about themes as data and privacy.

On a completely integrated smart campus, it is expected from the secondary analysis, that the behaviour of students will change through presence of technology. However, it is unknown how drastically this will change. If indeed a described amplification as surveillance capitalism (Zuboff, 2019), a data-dictatorship scenario (Van Loenen & Ploeger, 2018), a darkening of the digital dream dramatization (Zuboff, 2019), or the concepts of a prescriptive city (Sennet, 2018) does exist within this research, is difficult to deduce from this research. These concepts are extremes and should be nuanced. However, what is illustrated by this research is the importance to consider these extremes in the process of integration of technology in our society and to imagine what could be the effects on society and users in the long term. Features that should be taken into consideration within this process, according to this research, are clear governance, transparency about purposes of data collection and the process of data collection itself, presence of a trusted party that processes the data, and controllability of personal data for citizens.

Further research is needed to examine what a smart city means for the behaviour of citizens on the ground level. There are many useful purposes of technology that could be implemented within a city, such as for purposes of participation stimulation and democratization, as stated by Sennet (2018). These useful purposes appear in the data-democracy scenario (Van Loenen & Ploeger, 2018) and the coordinative smart city, as described by Sennet (2018). Furthermore, Sennet (2018) and Hajer (2014) state that it is prudent that technology stimulates the benefits from urban environments, such as serendipity and creativity. With these stimulations, zero-friction enclaves are avoided and growth is encouraged by including the possibility to make errors (Hajer 2014). These stimulations are beneficial for the liveability of an urban environment.

When these suggestions are put into perspective of the Sidewalk labs project at the Toronto Waterfront, it is understandable that the project must deal with such high resistance. The media and critics report about privacy concerns (BBC, 2019; Peel & Tretter, 2019), it is unclear what data is monitored and it is unclear for what purposes the data is used. Moreover, the project is not aimed at a bottom-up system wherein participation is considered important. A city does not necessarily improve if sensors are put on every street corner. Goals of monitoring every citizen and pursuing optimization are not expected to create urban growth or urban efficiency. Smart cities that implement technology that embraces urban profits such as participation, serendipity and face-to-face contact are far more democratic and liveable in the long term. Data and technology should be a means to an end, not an end in itself.

7. Discussion, limitations and recommendations

As Harari (2018) already calls for, we need to focus on the impact of technology in the 21st century. It is inevitable and without a doubt that technology will grow in importance. Technology can certainly improve liveability in cities by a properly designed policy for a smart city (Sennet, 2018). However, protection of personal data, and more generally, privacy in technology seems precarious and mutable in time and per situation. For example, individuals are willing to give up their privacy in exchange for health, while privacy is not about individual cases. Instead, this is about collective privacy and democracy, as described by Zuboff (2019). Zuboff (2019) believes that if people consider privacy as an individual case, the collective privacy is likely to erode. She states that the citizen itself will have less and less control. An illustration of what privacy erosion looks like is the well-known Chinese Social Credit System. Although it is unlikely today that such a system will be put into use in EU since it violates the GDPR (Autoriteit Persoonsgegevens, n.d.)., there are companies, such as google, that collect increasing amounts of data (Zuboff, 2019). Digitization has a huge impact on the lives of citizens and it increases the risk of loss of privacy (Ståhlbröst, Padyab & Hollosi, 2015). Therefore, this research recommends that privacy needs to be preserved in the development of smart campuses and smart cities. As already stated, the integration of technology is inevitable. Therefore, initiatives as BOLD cities, which aim at increasing user awareness and people as researchers, politicians and lawmakers are essential in the coming years (Centre for BOLD Cities, n.d.).

Admittedly, this research has its limitations. It is not a tight experiment that tests the effect of variable A on variable B. This is already shown in the statistical analysis. But specifically, this multifaceted and multidisciplinary research could not be embraced from a single perspective or variable. Either way, not in this current state of the development of a smart campus and a smart city. Hence, this research could be considered scientific since it examines the subject in an inductive way. A city interfaces with almost every field of research, which made this thesis so comprehensive. As a result, it is difficult to have conclusions with high certainty. The outcomes should more be interpreted as directives for policy. In order to have a more specific area of research, the campus of TU Delft was chosen to examine the smart city in miniature. With this scale-down, more in-depth information can be conducted and therewith, this information could be generalized to the larger scale of a smart city. Certainly, this is also a limitation to the research since cities and campuses vary widely. However, it is assumed that there are sufficient similarities to be able to generalize some conclusions from the campus to the city.

Besides these limitations, the bias of the researcher and the respondents surely contribute to the outcomes of the research. The processed literature and variables are undeniably influenced by the researcher's body of knowledge, the chosen scientific background and personal interests of the researcher. Besides, the chosen questions in the questionnaire are not directly derived from indisputable theory and assumptions. Not to mention the bias of the respondents that completed the questionnaire. They also have a specific view on the problem that may vary from citizens of a smart city. Besides the specific views on the problems, the fact that the students participated in the survey at all probably has to do with their bias. Although the sample selection was randomized, the possibility that the invitation for the survey is mostly accepted by students that have a better perception of privacy could not be

excluded. These possible biases of the student sample may affect the outcomes of this research since citizens with different biases may have a completely different perception of privacy.

Notwithstanding these limitations, this research provides a unique insight into the users' perspective on smart cities and smart campuses. Because of this thesis, people are set to thinking and are forced to have an opinion about topics that some individuals have never thought of. These kinds of processes, that create awareness, enable people to have a critical view of data and technology and to prevent inequality of power and knowledge. The movement of critical people hopefully results in informed decisions with all the implications well thought through.

Even more, attention to this subject is important in this COVID-19 crisis that the world is facing right now. Hereby, people are rapidly dependent on technology and digitalization. Examples are corona applications that track social contacts, video conferences to work from home and spy software to have exams from home. The urge for research on the effects of technology on society is thus constantly growing. It helps people gain and regain control and independence of their data. Therefore, this strongly inductive research has value.

For further research, it is recommended to focus more on the association of variables and the coefficient of it. The variables need to be researched in a more isolated form. The users' and ground-level perspective should be examined further and more extensively. Moreover, more specific applications of technology for participation and democratization should be investigated.

Moreover, further research is needed for other groups in society. Only a small group of the total population of cities is researched. Besides that, campus users are not constantly on campus. Within the city this is different. The effects of constant monitoring and tracking should therefore also be examined. In addition, research is needed to find out how monitored people change behaviour and how they respond to it from a more psychological and sociological view. Does user-friendly technology make people in cities indeed become stupefied, as envisaged by Sennet (2018)?

In this thesis, the concept of perception is very comprehensive. Therefore, further research should narrow this down and specifically focus on awareness, concerns or other components of perception. Hereby, initiatives such as BOLD cities play a crucial role (Centre for BOLD Cities, n.d.). These initiatives should be further examined and expanded. More people should become more informed about their data and more aware of the data they share. This process of education and research to improve this is crucial for a user-empowered future.

8. References

Ackerman, M. S. et al. (1999), Privacy in E-commerce: Examining user scenarios and privacy preferences, in Proceedings of Electronic Commerce, pp 1-8

Agate, V., Concone, F., & Ferraro, P. (2018, June). WiP: Smart Services for an Augmented Campus. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 276-278). IEEE.

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

AMS Institute. (n.d.). Urban Challenges. Retrieved September 27, 2019, from https://www.ams-institute.org/urban-challenges/

Austin, D. M., Furr, L. A., & Spine, M. (2002). The effects of neighbourhood conditions on perceptions of safety. Journal of criminal justice, 30(5), 417-427.

Autoriteit Persoonsgegevens. (n.d.). De AVG in een notendop. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/notendop_avg.pdf

Banisar, D. & Davies, S. (1999). Privacy & human rights-an international survey of privacy laws and developments. The John Marshall journal of computer & information law.

Bargh, M. S., & Choenni, S. (2013). On preserving privacy whilst integrating data in connected information systems. In Proceedings of the International Conference on Cloud Security Management (ICCSM'13), Seattle, US, 17–18 October

Bates, O., & Friday, A. (2017). Beyond data in the smart city: repurposing existing campus IoT. IEEE Pervasive Computing, 16(2), 54-60.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., … Portugali, Y. (2012). Smart cities of the future. European Physical Journal: Special Topics, 214(1), 481–518. https://doi.org/10.1140/epjst/e2012-01703-3

Batty, M. (2013). Big data, smart cities and city planning. Dialogues in Human Geography, 3(3), 274–279. https://doi.org/10.1177/2043820613513390

BBC News. (2018, May 27). Google's city built 'from the internet up'. Retrieved October 30, 2019, from https://www.bbc.com/news/technology-41414872

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

Bélanger, F., Hiller, J., and Smith, W. J. (2002). "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," Journal of Strategic Information Systems (1 1:3/4), pp. 245-270

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. IEEE Pervasive computing, (1), 46-55.

Berthoud, R. (2000b). 'A Measure of Changing Health', in R. Berthoud and J. Gershuny (eds), Seven Years in the Lives of British Families: Evidence on the Dynamics of Social Change from the British Household Panel Survey. Bristol: Policy Press

BOSS. (n.d.). TU Delft Real Estate Management. Retrieved April 11, 2020, from https://www.bosstudelft.nl/5937-2/

Bryman, A. (2012). Social Research Methods (4th ed.). New York, United States: OUP Oxford.

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. *Journal of urban technology*, *18*(2), 65-82.

Centre for BOLD Cities. (n.d.). Centre for BOLD Cities - About us. Retrieved March 13, 2020, from https://www.centre-for-bold-cities.nl/about-us

Choenni, S., Bargh, M. S., Roepan, C., & Meijer, R. F. (2016). Privacy and security in smart data collection by citizens. In Smarter as the New Urban Agenda (pp. 349-366). Springer, Cham.

CityLab. (2019, June 27). A Big Master Plan for Google's Growing Smart City. Retrieved October 30, 2019, from https://www.citylab.com/solutions/2019/06/alphabet-sidewalk-labs-toronto-quayside-smart-city-google/592453/

Clarke, R. (1999). Roger Clarke's "Privacy Introduction and Definitions." Retrieved November 29, 2019, from http://www.rogerclarke.com/DV/Intro.html

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. The counseling psychologist, 35(2), 236-264.

Chen, Z., Jiang, C., & Xie, L. (2018). Building occupancy estimation and detection: A review. *Energy and Buildings*, *169*, 260-270.

Christensen, K., Melfi, R., Nordman, B., Rosenblum, B., & Viera, R. (2014). Using existing network infrastructure to estimate building occupancy and control plugged-in devices in user workspaces. *International Journal of Communication Networks and Distributed Systems*, *12*(1), 4-29.

Culnan, M.J. & Armstrong, P. K. 1999, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science, 10, 104 – 115.

Dalla Corte, L., Van Loenen, B., & Cuijpers, C. (Eds.). (2017). Personal data protection as a nonfunctional requirement in the smart city's development (-). Barcelona: Huygens Editorial.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents -measurement validity and a regression model. Behaviour and Information Technology, 23(6), 413–422. https://doi.org/10.1080/01449290410001715723

Edwards, L. (2016). Privacy, security and data protection in smart cities: A critical EU law perspective. *Eur. Data Prot. L.* Rev., 2, 28.

European Court of Human Rights. (2019, August). *Guide on Article 8 of the European Convention on Human Rights*. Retrieved from https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

EU. (2016). Official Journal of the European Union (L 119/88). Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/gdpr.pdf

Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments. Science and Public Policy, 40(6), 717-723.

Grissa, M., Hamdaoui, B., & Yavuza, A. A. (2017). Location privacy in cognitive radio networks: A survey. IEEE Communications Surveys & Tutorials, 19(3), 1726-1760.

Griffioen, S., Vermeer, M., Dukai, B., Spek, S. V. D., & Verbree, E. (2017). Exploring indoor movement patterns through eduroam connected wireless devices. In A. Bregt, T. Sarjakoski, R. V. Lammeren, & F.

Rip (Eds.), Proceedings of the 20th AGILE Conference on Geographic Information Science: Societal Geoinnovation Wageningen University.

Hajer, M. A. (1999). Zero-friction society. *Urban Design*, *71*.

Hajer, M., & Dassen, T. (2014). *Smart about cities: visualizing the challenge for 21st century urbanism*. Rotterdamnai010 publishers.

Harari, Y. N. (2018). 21 lessons for the 21st century. First edition. New York: Spiegel & Grau

Huisman, O., & De By, R. A. (2009). Principles of Geographic Information Systems: An Introductory Textbook (1st ed.). Retrieved from https://webapps.itc.utwente.nl/librarywww/papers_2009/general/PrinciplesGIS.pdf

Junglas, I. A., & Watson, R. T. (2008). Location-based services. Communications of the ACM, 51(3), 65.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64(2013), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kugler, M. B., & Strahilevitz, L. J. (2016). Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory. *The Supreme Court Review*, *2015*(1), 205-263.

Liang, Y., Cai, Z., Han, Q., & Li, Y. (2017). Location privacy leakage through sensory data. Security and Communication Networks, 2017.

Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136-141.

Musa, A. B. M., & Eriksson, J. (2012, November). Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of the 10th ACM conference on embedded network sensor systems* (pp. 281-294).

Naafs, S., & Ettema, O. (2017, December 6). De muren hebben sensoren. De Groene Amsterdammer, 2017(49). Retrieved from https://www.groene.nl/artikel/de-muren-hebben-sensoren

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Niemtus, Z. (2019, 22 februari). Are university campuses turning into mini smart cities? The Guardian. Retrieved from https://www.theguardian.com/education/2019/feb/22/are-university-campuses-turning-into-mini-smart-cities

Peel, K., & Tretter, E. (2019). Waterfront Toronto: Privacy or Piracy? UCCities Working Paper # 2. DOI: 10.31235/osf.io/xgz2s

Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure, Albany: State University of New York Press.

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? IFIP Advances in Information and Communication Technology, 298(216483), 226–236. https://doi.org/10.1007/978-3-642-03315-5_17

Preacher, K. J. (2001). Calculation for the chi-square test: An interactive calculation tool for chi-square tests of goodness of fit and independence [Computer software]. Available from http://quantpsy.org.

Roche, S., & Rajabifard, A. (2012). Sensing places' life to make city smarter. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 41–46. https://doi.org/10.1145/2346496.2346503

Roche, S. (2014). Geographic Information Science I: Why does a smart city need to be spatially enabled? Progress in Human Geography, 38(5), 703–711. https://doi.org/10.1177/0309132513517365

Sennett, R. (2018). *Building and dwelling: ethics for the city*. Farrar, Straus and Giroux.

Ståhlbröst, A., Padyab, A., Sällström, A., & Hollosi, D. (2015). Design of Smart City Systems from a Privacy Perspective. IADIS International Journal on WWW/Internet, 13(1), 1–16.

Sidewalk Labs. (2019). Toronto Tomorrow (A new approach for inclusive growth). Retrieved from https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/23135500/MIDP_Volume0.pdf

Simmons, R. (2019). *Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century.* Cambridge: Cambridge University Press. doi:10.1017/9781108692939

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly, 167-196.

Song, H., Fink, G. A., & Jeschke, S. (2017). Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. Hoboken, USA: Wiley.

SurveyMonkey. (n.d.). Sample Size Calculator: Understanding Sample Sizes. Retrieved April 20, 2020, from https://www.surveymonkey.com/mp/sample-size-calculator/

TU Delft. (2019). Facts & Figures. Retrieved from https://d1rkab7tlqy5f1.cloudfront.net/TUDelft/Over_TU_Delft/Feiten_Cijfers/jaarverslagen/opmaak%20facts%20%26%20figures%202018%20lr.pdf

TU Delft. (n.d.). Historie - Campus Development. Retrieved November 10, 2019, from https://campusdevelopment.tudelft.nl/historie/

TU Delft. (2019, January 7). Studentenpopulatie. Retrieved April 20, 2020, from https://www.tudelft.nl/over-tu-delft/feiten-en-cijfers/onderwijs/studentenpopulatie/

TU Delft. (2020, April 17). Gebouwen. Retrieved April 20, 2020, from https://iamap.tudelft.nl/bereikbaarheid/gebouwen/

TU Delft. (2020). *Facts & Figures 2019/2020*. Retrieved from https://d1rkab7tlqy5f1.cloudfront.net/TUDelft/Over_TU_Delft/Feiten_Cijfers/jaarverslagen/facts%20%26%20figures%202019%20web.pdf

TU Delft. (n.d.). Smart Buildings: from detached technology to an integral, smart system. Retrieved March 3, 2020, from https://www.tudelft.nl/en/sustainability/campus/smart-buildings/

TU Delft Library. (2016, May). *TU Delft Data Stewardship Policy Framework* (1.0). Retrieved from https://pure.tudelft.nl/portal/files/51438802/IndoorMovementThroughEduroam_1.pdf

Valks, B., Arkesteijn, M., Den Heijer, A., & Putte, H. V. (2016). Smart campus tools: een verkenning bij Nederlandse universiteiten en lessen uit andere sectoren (report commissioned by DFB). *Delft: TU Delft*.

Valks, B., Arkesteijn, M., & den Heijer, A. (2018). Smart campus tools 2.0: An international comparison. Delft University of Technology.

Valks, B., Arkesteijn, M., & den Heijer, A. (2019). Smart campus tools 2.0 exploring the use of real-time space use measurement at universities and organizations. Facilities. https://doi.org/10.1108/F-11-2018-0136

Van der Hoeven, F. (2015). Campus Delft: History, policy framework and development of the TU Delft campus. Project Baikal, 12(44), 152–159. https://doi.org/10.7480/projectbaikal.44.854

Van Loenen, B., & Ploeger, H. (2018). 2050: The Story of Urbidata. In B. van Loenen, G. Vancauwenberghe, & J. Crompvoets (Reds.), Open Data Exposed (pp. 269–288). The Hague, The Netherlands: T.M.C. Asser Press.

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

Vasileva, R., Rodrigues, L., Hughes, N., Greenhalgh, C., Goulden, M., & Tennison, J. (2018). What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data. *Information*, *9*(10), 251.

Villares, M. (2016, July 4). *TU Delft Campus* [Illustration]. Retrieved from https://www.delta.tudelft.nl/article/campus-qualities-and-landmarksWarren, S. D., & Brandeis, L. D. (1890). Right to privacy. Harv. L. Rev., 4, 193.

Westin, A. F. (1967). *Privacy and freedom* (1st ed.). New York: Atheneum.

Zhou, T. (2017). Understanding location-based services users' privacy concern: an elaboration likelihood model perspective. Internet Research, 27(3), 506-519.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, United States of America: Public Affairs, Hachette Book Group.

Zuboff, S. (2020, February 27). U wordt nú gecontroleerd. *De Groene Amsterdammer*, *144*(9), 26–31.

Appendices

Appendix A: Analysis scheme

In this analysis scheme, the questions are the manifest variables and the underlying concepts are the latent variables. Only the questions with comparable scales and researched concepts are included in these analyses. The other questions are focused on the comparison of means or only to research the distribution of the opinions of the students.

Before concepts are analysed to find correlations between them, a factor analysis should give insight about what manifest variables measure what latent variables. It is required for the correlation that the manifest variables measure one single latent variable or component. Besides that, the factor analysis is very suitable for the reduction of dimensions. After the components are extracted, the components' reliability is tested. If the components are unreliable, then they are only suitable for comparison of means.

Correlation analysis

For correlation, the aggregated latent variables are suitable, according to the factor analysis and the reliability analysis. Furthermore, single questions are also included in some cases. The components that are used for correlation are the computed variables 'concerns', 'knowledge of privacy security', ''ability to control data of online behaviour on campus', 'comfortability of being tracked' and 'acceptability of data-use of online information on campus'. The non-computed variable is 'ability to control data of offline behaviour on campus'.

The correlation analysis aims to find relationships between variables (Bryman, 2012). These relationships are expressed in a value between -1 and +1. The closer the coefficient is to -1 or +1, the stronger the relationship is. If the relationship is close to 0, the relationship is weak. A negative coefficient means a negative relationship and a positive coefficient means a positive relationship. The interpretation of the strength of the relationships is shown in table 33. The correlation is expressed in Spearman's Rho if the variables are ordinal and in Pearson's Rho if the variables are scale. The correlation is expressed in Cramer's V if the variables are nominal. However, the Cramer's V only gives the strength of the relationship and not the coefficient. Therefore, Cramer's V has a value of 0 to 1. In the survey analysis, only significant correlations are included in the results chapter.

Table 33 (Source: Lee, D. (2016))

Estimated values	Interpretation of association
0.00–0.10	Negligible
0.10–0.20	Weak
0.20–0.40	Moderate
0.40–0.60	Relatively strong
0.60–0.80	Strong
0.80–1.00	Very strong

Factor and reliability analysis

Cronbach's Alpha measures internal reliability of the questions in the survey (Bryman, 2012). Questions in the survey could be unreliable by design or through false interpretation of the respondent. Besides reliability, Cronbach's Alpha also measures consistency of Likert-scaled questions. The value of Cronbach's Alpha varies between 0.0 and 1.0, whereby 0 is unreliable and 1 is reliable. Berthoud (2000), states that a minimum level of 0.60 is described as 'good'.

Q10

In Q10, students' general privacy concerns for data usage for real-time measurement are measured. This latent variable is divided in four different manifest variables, which are concerns of usage by the government, the university, advertisers/commercial parties and commercial parties on campus. The factor analysis shows in table 35, that these four different manifest variables explain 62,061% of the value (Eigenvalue>1). Furthermore, table 35presents that the manifest variables are explaining one component and that the variables are significant. This component is suitable for further analysis. Thereby, the manifest variables can be aggregated into one variable named 'concerns'.

Table 34

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,482	62,061	62,061	2,482	62,061	62,061
2	,738	18,451	80,513			
3	,475	11,887	92,399			
4	,304	7,601	100,000			

Extraction Method: Principal Component Analysis.

Table 35

Component Matrix[a]	Component 1
The government	,817
The university	,810
Commercial parties on campus	,790
Advertisers/Commercial services	,733

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

If the new variable is used for further analysis, a reliability analysis is required first. When Q10 is tested for internal consistency, Cronbach's Alpha is 0.796 with a n-value of 125. This question is thus reliable, according to table 36 and the new variable can be used for further analysis.

Table 36

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,796	,796	4

Q11

Q11 measures the latent variable of knowledge of privacy security. The students are asked about their knowledge of the content of the GDPR, the Privacy Statement of TU Delft and the privacy policies from other services they use on campus. These 3 variables are the manifest variables. The factor analysis calculates whether these questions measure one latent variable. In table 37 the factor analysis shows that these manifest variables together explain 66,523% of the variance (Eigenvalue>1). Furthermore, table 38 shows that all variables are significant. This implies that these manifest variables could be aggregated to one variable named 'knowledge of privacy security'.

Table 37

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1,996	66,523	66,523	1,996	66,523	66,523
2	,685	22,832	89,355			
3	,319	10,645	100,000			

Extraction Method: Principal Component Analysis.

Table 38

Component Matrix[a]	Component 1
How familiar are you with the content of the following? - The privacy statement of TU Delft	,876
How familiar are you with the content of the following? - Privacy policies from other services on campus	,865
How familiar are you with the content of the following? - The General Data Protection Regulation or GDPR (AVG in Dutch)	,693

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Before the new variable 'knowledge of privacy security' could be used for further analysis, a reliability analysis is required. A reliability analysis gives a Cronbach's Alpha of 0.702 in table 39 for a n-value of 125, which is acceptable. This new variable is suitable for further analysis

Table 39

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,702	,743	3

Q12

The latent variable of ability to control data is measured in **Q12**. This question consists of 4 manifest variables, which are data of location on campus, data of online behaviour on campus, data of service-usage on campus and data of offline behaviour on campus. When the factor analysis is done, table 40 shows that the four manifest variables explain two components. These two components together explain 75.519% of the variance (Eigenvalue>1). Furthermore, the significances are presented in table 41. This rotated component matrix shows that 'ability to control data of usage of services on campus' and 'ability to control data of online behaviour on campus' belong to one component. Besides, the matrix shows that 'data of offline behaviour on campus' belongs to another component. The manifest variable 'data of your physical location on campus' is not significant since the difference between both loadings in the components is less than 0.2. Therefore, this manifest variable is excluded and could be used only for a comparison of means. The two components that proceed are divided into 'ability to control data of online behaviour on campus' and 'ability to control data of offline behaviour on campus'

Table 40

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1,851	46,286	46,286	1,851	46,286	46,286
2	1,209	30,233	76,519	1,209	30,233	76,519
3	,559	13,963	90,483			
4	,381	9,517	100,000			

Extraction Method: Principal Component Analysis.

Table 41

Rotated Component Matrix[a]

	Component	
	1	2
Your usage of services on campus	,886	-,133
Your online behavior on campus	,847	,165
Offline behavior on campus (conversations)	-,153	,902
Your physical location on campus	,498	,656

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

In table 42, the Cronbach's Alpha for the latent variable 'ability to control data of online behaviour on campus' is showed. A reliability analysis for the other component of Q12 is impossible since the latent variable only consist of one manifest variable. For the latent variable 'data of online behaviour on campus' the Cronbach's Alpha is 0.733 with a n-value of 124. Therefore, the results of these questions can be described as reliable. The two components are suitable for further analysis.

Table 42

Reliability Statistics

Cronbach's Alpha	N of Items
,733	2

Q23

Q23 focuses on the comfortability of the students of being tracked. This latent variable is split up in 8 manifest variables that represent specific purposes of being tracked. These purposes are both derived from the secondary analysis and hypothetical. The factor analysis in table 48 shows that the 8 manifest variables explain one component or 46,365% (Eigenvalue>1). Therefore, these 8 manifest variables could be aggregated to one variable named 'comfortability of being tracked' as all manifest variables are significant, which is showed in table 44.

Table 43

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3,709	46,365	46,365	3,709	46,365	46,365
2	,950	11,880	58,245			
3	,751	9,392	67,637			
4	,723	9,032	76,669			
5	,615	7,690	84,360			
6	,517	6,462	90,821			
7	,491	6,133	96,954			
8	,244	3,046	100,000			

Extraction Method: Principal Component Analysis.

Table 44

Component Matrix[a]

	Component
	1
To navigate (e.g. to lecture room, to bus stop)	,824
For study services (printing, finding available workplaces)	,759
For research	,734
For offering personal services (e.g. psychological consult, finding a workplace)	,689
For being stored	,646
For targeted advertisements	,627
For measuring your study progress (e.g. presence)	,576
To sell it to third parties	,545

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Again, the latent variable 'comfortability of being tracked' is tested for reliability before it could be used for further analysis. Table 45 presents the Cronbach's Alpha for a n-value of 107. This Cronbach's Alpha is 0.83, which means that this Likert-scale question is highly reliable and internal consistent. Hence, this component can be included in further analysis.

Table 45

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,828	,831	8

Q24

The latent variable 'acceptability of usage of personal data on campus' is also divided in 8 manifest variables that consist of various types of personal data. These manifest variables are processed in Q24. The factor analysis is table 46 show that these 8 manifest variables explain three components for 63,449% (Eigenvalue>1). This means that 3 concepts are measured and that these 8 variables are not suitable for aggregation. Table 47 shows which variables belong to which component, included their loadings. One variable is not significant because it belongs to two components and the difference is less than 0.2. This is the variable 'your activities'. This variable is excluded from further analysis and is only presented as a comparison of means. The three components are divided in 'wellbeing and participation', 'bodily information' and 'online information'. These components are further included in the analysis.

Table 46

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,426	30,326	30,326	2,426	30,326	30,326
2	1,374	17,171	47,497	1,374	17,171	47,497
3	1,276	15,951	63,449	1,276	15,951	63,449
4	,792	9,901	73,350			
5	,629	7,858	81,208			
6	,621	7,762	88,969			
7	,513	6,408	95,378			
8	,370	4,622	100,000			

Extraction Method: Principal Component Analysis.

Table 47

Rotated Component Matrix[a]

	Component		
	1	2	3
Your emotional well-being (e.g. e-consult of a psychologist)	,760	,164	
Your study participation (e.g. presence in lectures)	,735	-,255	,267
Your activities (e.g. study, sport, leisure)	,604	,425	
Your offline behavior (e.g. conversations)	-,177	,756	
Your biometric information (heart rate, fingerprint)	,437	,699	
Your location	,127	,654	
Your online behavior (e.g. browser history)	-,108		,875
Your transactions (e.g. payments in shops)	,279	,112	,797

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 5 iterations.

The three components are tested for reliability and internal consistency. The three Cronbach's Alphas with a n-value of 106 are presented in table 48, 49 and 50. The Cronbach's Alpha for the first component 'wellbeing and participation' is 0.501 and is not reliable. The second component 'bodily information' has a Cronbach's Alpha of 0,457 and is also not reliable. The Cronbach's Alpha for the third component 'online information' is slightly reliable with a value of 0.611. Hence, the only component that is suitable for further analysis is 'acceptability of data-use of online information on campus'. The other components are only suitable for a comparison of means.

Table 48

Reliability Statistics

Cronbach's Alpha	N of Items
,501	2

Table 49

Reliability Statistics

Cronbach's Alpha	N of Items
,457	3

Table 50

Reliability Statistics

Cronbach's Alpha	N of Items
,611	2

Reliability analysis for multiple choice questions: Q7, Q9, Q13, Q14

Cronbach's Alpha is also used for the determination of internal consistency of multiple-choice questions. The value gives feedback on how much the questions hang together. Hereby, the various manifest variables measure one latent variable. In Q7, these manifest variables concern activities of students on campus. This question should give insight in the type of activities on a campus and should provide insight how multifunctional a campus is. As can be seen in table 51, the Cronbach's Alpha value is 0.852 with a n-value of 145. This Cronbach's Alpha value implies a high internal consistency for this question. None of the activities should be excluded according to table 52.

Table 51

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,852	,855	9

Table 52

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Attend_lectures	3,19	4,495	,406	.	,851
Self_study	3,29	4,099	,494	.	,844
Group_work	3,21	4,384	,443	.	,848
Eating	3,64	3,431	,705	.	,823
Sports	3,65	3,427	,709	.	,822
Work	3,95	3,847	,667	.	,826
Leisure	3,99	3,973	,659	.	,828
Living	4,01	4,109	,622	.	,833
Other	4,05	4,392	,509	.	,844

In Q9, the devices that people use that can be detected on campus are questioned. Device-use is the latent variable here, that is measured by 5 manifest variables. This question gives insight in the uses of devices from campus users, which is important since users' data is crucial for a smart campus and a smart city to function. As shown in table 53, the Cronbach's Alpha is 0.578 with a n-value of 145. This means that this question should be considered as internal inconsistent. These manifest variables do not give a sufficient determination of the latent variable. Therefore, this question is not further analysed in the results chapter. As already can be seen from the results of this question, smartphones and laptops are used by roughly anyone and that desktops are used by 38%. The other devices, as presented in the question, are rarely or not used.

Table 53

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,578	,622	5

Q13 concerns perception of methods of detection. Hereby, students are asked per method of detection, which are the 7 manifest variables, if they think they can be detected by this. Perception of detection is the latent variable. Table 54 and 55 give a Cronbach's Alpha of 0.767, which implies an internal consistent question with a n-value of 120.

Table 54

Reliability Statistics

Cronbach's Alpha	N of Items
,767	7

Table 55

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Wi_Fi	1,73	2,470	,176	,782
Bluetooth	2,33	1,499	,711	,681
RFID	2,01	1,689	,562	,724
Camera_detection	2,21	1,444	,734	,674
Infrared	2,63	2,119	,510	,739
Wearable_sensors	2,63	2,119	,510	,739
Other1	2,68	2,454	,277	,775

The current use of smart campus tools by students is measured in Q14. Hereby, usage of smart campus tools is the latent variable that is measured by 6 manifest variables. Table 56 and 57 present a very high Cronbach's Alpha of 0.903 which means that this question has a very high internal consistency with a n-value of 119.

Table 56

Reliability Statistics

Cronbach's Alpha	N of Items
,903	6

Table 57

For which of the following situations do you use tools on campus that are provided by the university? Multiple answers possible.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
To find an available PC workplace (desktop)	1,46	3,172	,771	,883
To find an available study space without a PC	1,44	3,101	,789	,880
To book a project room	1,06	2,996	,574	,916
To book a study place	1,28	2,744	,833	,870
. Indoor navigation	1,47	3,278	,725	,890
I don't use tools for any of these situations	1,26	2,733	,819	,872

Appendix B: Survey

Privacy of geographical data in the smart campus of TU Delft

Welcome to the survey about privacy of personal information in smart cities and smart campuses
First of all, thank you for agreeing to take part in this survey!
My name is Tom Molenaar and I am a MSc. Geographical Information and Management Applications (GIMA) student at Utrecht University.
For my thesis I research one of most debatable topics of the present and the near future. In my research, which I carry out under the department of Urbanism at TU Delft, I want to find out how people see our digital future and how people see themselves in this digital era, and more specifically the data driven city: the smart city.

Smart cities (and as part of city, a smart campus) are often described concepts that strongly relates to our digital future. These concepts are mostly described, researched and explained from a technical point of view: the data collection, the data management and the services provided by use of these data. My research focuses on the user perspective: where do users place themselves in these smart cities? I conduct this survey to answer this question and to contribute to the public-political debate.
In this survey, I analyse the perception of users on the TU Delft Campus. The TU Delft Campus aims to become a so-called Smart Campus. A Smart Campus works with real-time space use measurements to improve the effective and efficient use of buildings and space. These real-time space use measurements mostly consist of (location) information from users of the campus, which means that this information is crucial for a smart campus to function.

Since you are a user of the Campus, I hope to gain information about your perception of privacy on campus in regard to the personal data that you share with others for real-time space use measurements. Furthermore, I am questioning your thoughts about a future smart campus. Via this survey you can give your opinion and contribute to my thesis.

This survey should take about 10 minutes to complete.
Be assured that all answers you provide will be kept confidential and anonymous.
If there are any questions or if you are interested and want to know more, please contact me.
t.b.molenaar@student.tudelft.nl

Q1 What is your age?

- ○ Under 18
- ○ 18 - 20
- ○ 21-23
- ○ 24-26
- ○ 27 years or older

Q2 What is your gender?

- ○ Male
- ○ Female
- ○ Other
- ○ I prefer not to say

Q3 At what university are you enrolled?

- ○ TU Delft
- ○ University of Utrecht
- ○ Other Dutch university
- ○ University outside the Netherlands

Q4 What type of degree is your study?

- ○ Bachelor's degree
- ○ Master's degree
- ○ Doctorate
- ○ Other

Q5 What do you study?

_____

Q6 What year did you start this study?

- ○ before 2016
- ○ 2016
- ○ 2017
- ○ 2018
- ○ 2019

Q7 Which activities do you usually do on campus at TU Delft? Multiple answers possible.

- ☐ Attend lectures
- ☐ Self-study
- ☐ Group work/projects
- ☐ Eating (kiosks/restaurants/bar)
- ☐ Sports
- ☐ Work
- ☐ Leisure
- ☐ Living (Duwo housing)
- ☐ Other

_____

Q8 How often do you go to the campus at TU Delft in a regular week?

- ○ Less than once a week
- ○ once a week
- ○ 2 times a week
- ○ 3 times a week
- ○ 4 times a week
- ○ 5 times a week
- ○ More than 5 times a week

Q9 What devices that can be detected on campus do you use on campus at TU Delft? Multiple answers possible.

- ☐ Mobile phone
- ☐ Laptop
- ☐ Tablet
- ☐ Computer from university (desktop)
- ☐ Smartwatch
- ☐ Other devices

_____

Q10 How concerned are you about your location information if this is used for real-time measurements by the following organisations?

	Very unconcerned	unconcerned	neutral	concerned	very concerned
The government	○	○	○	○	○
The university	○	○	○	○	○
Advertisers/Commercial services (Google, OV9292, Facebook etc.)	○	○	○	○	○
Commercial parties on campus (restaurants/bars/kiosk/shops)	○	○	○	○	○

Q11 How familiar are you with the content of the following?

	Not at all familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
The General Data Protection Regulation or GDPR (AVG in Dutch)	○	○	○	○	○
The privacy statement of TU Delft	○	○	○	○	○
Privacy policies from other services on campus	○	○	○	○	○

Q12 How do you perceive the ability to control access to the following types of personal data?
In the GDPR (AVG), personal data is defined as any information relating to an identified or identifiable natural person. This

information can be a name, ID-number, location information or physical, psychological, genetic, mental, economic, cultural of social information.

	Fully out of control	Out of control	Neutral	In control	Fully in control
Your physical location on campus	○	○	○	○	○
Your online behaviour on campus	○	○	○	○	○
Your usage of services on campus	○	○	○	○	○
Offline behaviour on campus (conversations)	○	○	○	○	○

Q13 Via several methods the university is able to detect your presence on campus territory. Via what of the following connection methods do you think you disclose your presence on campus? Multiple answers possible.

- ☐ Wi-Fi
- ☐ Bluetooth
- ☐ RFID (e.g. your student card to access doors)
- ☐ Camera detection
- ☐ Infrared
- ☐ Wearable sensors
- ☐ Other _____

Q14 For which of the following situations do you use tools on campus that are provided by the university? Multiple answers possible.

- ☐ To find an available PC workplace (desktop)
- ☐ To find an available study space without a PC
- ☐ To book a project room
- ☐ To book a study place
- ☐ Indoor navigation
- ☐ I do not use tools for any of these situations

Q15 Do you think you are sharing your location information with the university when you are on campus?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q16 Are you aware of what specific information you share on campus?

- ○ Very unaware
- ○ Unaware
- ○ Neutral
- ○ Aware
- ○ Very aware

Q17 How much do you feel you understand what the university is doing with your personal data?

- ○ Nothing
- ○ Very little
- ○ Some
- ○ Much

Q18 How would you describe your current ability to control (rectify/turn off) your location information that you share with the university when you are on campus?

- ○ Fully out of control
- ○ Slightly out of control
- ○ Slightly in control
- ○ Fully in control

Q19 How do you perceive your potential risk of losing information or misuse when you share information with the university when you are on campus?

- ○ Low risk
- ○ Moderately low
- ○ Moderate
- ○ Moderately high
- ○ High risk

Q20 Are you selective in sharing your location information on campus? (e.g. do you turn your GPS off?)

- ○ Yes
- ○ No

Q21 How are you selective in sharing your location information on campus?

_____

Q22 In level of safeness, how would you describe your current perception of the protection of personal data on campus?

- ○ Very unsafe
- ○ Unsafe
- ○ Neither safe nor unsafe
- ○ Safe
- ○ Very Safe

What follows are questions about smart campus tools in development and questions about how you see a smart campus in the future. This information will be used to be able to research the attitude of users towards a smart campus and ultimately a smart city. These attitudes from the respondents will contribute to the ongoing debate of what a smart campus and a smart city should look like.

Q23 How comfortable would you be if your personal data on campus is used, without specifically stated for what purpose this is used, for the following?

	Very uncomfortable	Uncomfortable	Neutral	Comfortable	Very comfortable
For measuring your study progress (e.g. presence)	○	○	○	○	○
To navigate (e.g. to lecture room, to bus stop)	○	○	○	○	○
For study services (printing, finding available workplaces)	○	○	○	○	○
For targeted advertisements	○	○	○	○	○
For offering personal services (e.g. psychological consult, finding a workplace)	○	○	○	○	○
For research	○	○	○	○	○
To sell it to third parties	○	○	○	○	○
For being stored	○	○	○	○	○

Q24 What of the following would you find acceptable if this is tracked on a smart campus?

	Unacceptable	Acceptable	Neutral
Your study participation (e.g. presence in lectures)	○	○	○
Your location	○	○	○
Your activities (e.g. study, sport, leisure)	○	○	○
your biometric information (heart rate, fingerprint)	○	○	○
your emotional well-being (e.g. e-consult of a psychologist)	○	○	○
Your transactions (e.g. payments in shops)	○	○	○
Your online behaviour (e.g. browser history)	○	○	○
Your offline behaviour (e.g. conversations)	○	○	○

Q25 What would you think if your location information on campus would also be used for commercial purposes such as food consumption and advertisements?

- ○ Unacceptable
- ○ Slightly unacceptable
- ○ Neutral
- ○ Slightly acceptable
- ○ Acceptable

Q26 Would you still use these tools if not the university but a commercial would take care of the smart campus?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q27 Currently, on some Dutch universities, cameras are used to monitor students' occupancy in lecture rooms. Would you mind to disclose your presence if this is used for the purpose of improving education?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q28 Another tool is a sensor under a desk at a working space that detects if the desk is occupied. Do you mind that your presence can be detected by these sensors if it becomes easier to find a free desk?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q29 Wi-Fi tracking is also used within Dutch universities to monitor movements of people on campus and to find out what places are often used and what places are less used. Would you disclose your personal information if your data is used for efficient use of the campus?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q30 Quantified Student is an application in development that aims to create a better learning experience for students. For this application, biometric information will be tracked, such as hours of sleep and level of stress. Besides that, other data as time on campus, alcohol consumption and study time is also tracked. If this application would be available for you in exchange for your information, would you use it?

- ○ Definitely not
- ○ Probably not
- ○ Might or might not
- ○ Probably yes
- ○ Definitely yes

Q31 I am willing to disclose my location information if this helps the functioning of space on campus.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Q32 How do you see your effort of protecting your location information on a (smart) campus in five years, in comparison to your current effort?

- ○ Much higher
- ○ Moderately higher
- ○ Slightly higher
- ○ About the same
- ○ Slightly lower
- ○ Moderately lower
- ○ Much lower

Q33 Why do you see your effort to protect your location information become higher?

_____

Q34 Why do you not see your effort to protect your location information become higher?

_____

Q35 What would you think of the TU Delft as a full 'smart campus' where everything is real-time tracked in regard to the protection of your personal information?

- ○ Very undesirable
- ○ Undesirable
- ○ Neither desirable nor undesirable
- ○ Desirable
- ○ Very desirable

Q36 How would you perceive the ability to control your personal data in a smart campus in five years?

- ○ Fully out of control
- ○ Slightly out of control
- ○ Slightly in control
- ○ Fully in control

Q37 How much do you expect to benefit from the personal information that you share with the smart campus?

- ○ None
- ○ Very little
- ○ Some
- ○ A great deal

Q38 In your opinion, what is most essential to safeguard user's personal information on a smart campus?

- ○ Users awareness of protecting personal information
- ○ Laws from the government
- ○ Measures taken by the smart campus itself
- ○ None of the above

End of the survey