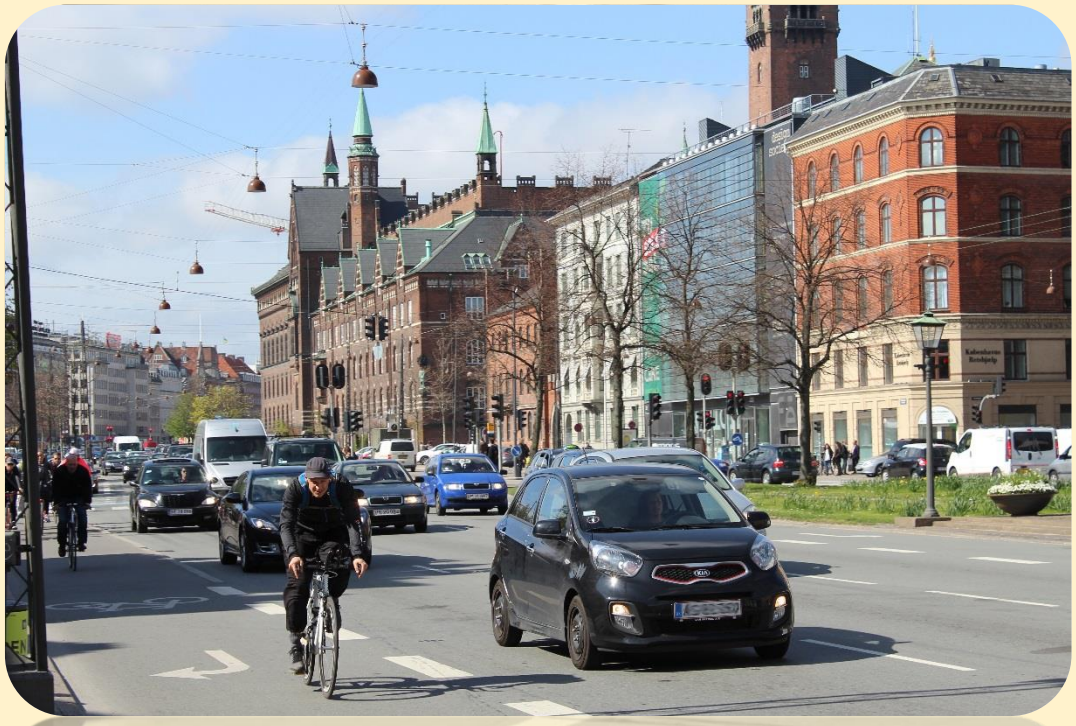
Sustainability and Data Collection in the Smart City

-A Case Study on the Wi-Fi and Bluetooth Tracking Project in Copenhagen



ARVIN GHASEMI, 2015
MVEM30 MASTER THESIS 30 HP
Applied Climate Change Strategies | Lund University

Sustainability and Data Collection in the Smart City

- A Case Study of the Wi-Fi and Bluetooth Tracking Project in Copenhagen

Arvin Ghasemi

2015

Supervisor: Stefan Larsson, Lund University Internet Institute (LUII)

LUNDS UNIVERSITET

Abstract

Cities around the world are facing a multitude of urban challenges that demand that they change the way they plan and think about their city, with one of the ways of approaching sustainability being the *Smart city*. A core feature of the Smart city is the idea of collecting large quantities of data on the city, *big data*, which is then used in various city solutions. In the wake of this, several questions dealing with sustainability surface and some of them are: transparency, privacy, citizen involvement and choice. The aim of this study is to investigate these and the smart city strategy by doing a case study of Copenhagen and the Wi-Fi and Bluetooth tracking project that started in 2014. Classic theories of surveillance such as Foucault's Panopticism are used to further deepen the analysis. The results show that the Wi-Fi tracking project is a part of Copenhagen's Intelligent Traffic System (ITS) program and collects the MAC addresses from the smartphones of citizens moving through the project area with activated Wi-Fi or Bluetooth. As this is done without the consent of citizens, the legality of the project is questioned. As for privacy, there seems to have been a change in the debate in and around the municipality, however the communication of the Smart city strategy to the citizens remains unchanged. The study concludes that Copenhagen has been shown to focus more on climate change, with their goal of being CO_2-neutral to 2025, private business partnerships, and the digital infrastructure in the form of the vision of Copenhagen Connecting, and less on citizen participation and choice in this transformation, in contrary to much of the Smart city theory. This study has contributed to the topic by giving some insight into the process of creating a Wi-Fi and Bluetooth tracking system within a Smart city strategy, and some of the issues that can surface when establishing such a system.

Keywords:

Smart City, Sustainability, Strategy, Wi-Fi tracking, Copenhagen, Privacy, Citizen Involvement and Participation, Surveillance

Contents

1. Introduction

Cities around the world are growing and changing, with no sign of the rapid urbanisation to decrease. On the contrary, in 2050 it's estimated that 66 % of the world's population is urban, an increase of 2.5 billion urban citizens compared to 2014 (UN, 2014). One of the challenges of this development is to not only keep these cities from getting crowded and inefficient, but to actually create better and more liveable cities. With this purpose in mind, visions of desirable future cities started to develop and spread among city planners and strategists' across the world, some of them called sustainable, green and others smart. While many of them focus on increasing the environmental performance and decreasing the global warming effect of the city, few have the focus on information and communication technology (ICT) that the Smart city has. Apart from this ICT focus, the Smart city encases many characteristics aimed at different urban challenges, such as mobility, climate mitigation and adaptation, social sustainability and resource efficiency. Cities can choose to address these differently and with varying importance and priority, depending on what the goals of the city are. The ICT focus of the smart city doesn't only mean large investments on technologic functions that benefit the city, but more specifically - the pursuit of data. In this context, more data is typically presented as better data, as it will result in improved decision-making. Logically, more data implies more collecting, and the ways of collecting data are constantly evolving, from traditional human administered car-counting on paper, to collecting via wireless protocols that are functioning around the clock with unlimited storage capabilities. It is when these high technological systems for collecting data are expanding, that the risk of collecting sensitive personal data increases. Of course, what we see as personal or sensitive data is relative and therefore it can be hard to know where privacy begins and ends. One of the privacy concerns that this thesis mainly deals with, is the disclosure of a person's physical location. In a survey conducted in the US; 50 % said that details of their physical location over time is "very sensitive" and 32 % answered "somewhat sensitive" (Pew Research Center, 2014). The remaining 16 % said that their physical location is "not too sensitive" or "not at all sensitive". This means that, at least to some people, the collection of their physical location over time *is* sensitive and an infringement of their privacy. This thesis will dive into the Smart city strategy of Copenhagen, and its use of Wi-Fi and Bluetooth tracking as a tool to reach their sustainability goals.

1.1. Environmental Relevance

The Smart city strategy is a way for Copenhagen to address the various urban challenges they face, as explained in the previous paragraph, but it can be manifested in different ways. Copenhagen has committed to a target to become the world's first carbon neutral capital by 2025, which can be seen as an indication of how seriously Copenhagen see the issue of climate change. So in this case the Smart city is a climate-strategic approach to creating a more developed city, and the Wi-Fi and Bluetooth tracking is created as a "smart" solution to parts of the issue of climate change.

In a more and more digital world, not only the sustainability of the physical aspects of the environment, economy and social world should be in the research spotlight, but also those that are not physical. While environmental science tends to look at the physical environment, the development of modern urban areas, through climate strategy or urban planning, should also consider the unphysical elements of the city, one of which is the digital infrastructure it contains and creates. This can be called the effort of digital sustainability, and should balance and complement the (analogue) physical sustainability. When it comes to urban data collection methods - the way we collect data in the city — it will affect the way that we deal with urban challenges based on that data. So, digital sustainability affects the physical sustainability, and this study aims to analyse some of the interaction between these two.

1.2. Purpose and Research Questions

One side of the sustainability strategy called the Smart city is the idea of collecting large quantities of data, *big data*, which is then used in various city solutions. In the wake of this, several questions dealing with sustainability surface and some of them being; transparency, privacy, citizen involvement and choice. The aim of this study is to investigate these by doing a case study of Copenhagen and the Wi-Fi and Bluetooth tracking project that started in 2014. The raised aspects will be balanced by presenting the benefits and opportunities of this project that are described by the municipality, and the idea of a digital infrastructure, called Copenhagen Connecting. Surveillance theories will enable a concretion of what a surveillance system contains, which then can be used to analyse the case. The research questions, which are focused on the case, are as follows:

- How is Copenhagen working with the Smart city strategy and what are some of the issues that are associated with this strategy?
- How does the Wi-Fi and Bluetooth tracking system of Copenhagen work?
- How aware is the municipality of the aspects of privacy and integrity?

- How does the tracking project and the smart city strategy of Copenhagen address citizen involvement and participation?

1.3. Disposition

This thesis is divided into 6 chapters, with the first being the introduction (1), followed by: an account of the case study methodology (2), the sustainability and smart city strategies (3), theories of surveillance (4), results of the study and analysis of the case (5) and lastly a discussion of the study (6).

2. Case Study Methodology

When a study is conducted there are many factors that affect the direction of the research and if it goes the direction that the researcher wants. To keep the study from drifting off from the original purpose, the methodology should be clear and articulate, not only to the researcher but also to the reader. This chapter aims to do just that; describe the design of the case study, the material and sources used and how the theory will be used.

While defining what a case study is can be a tiresome task (Gerring, 2007), generally it can be said to be an "intense examination of a single case of a particular phenomenon" (Orum, 2001 p.1509). This can be expanded to making comparisons to similar or different cases as well, though that is not the case for the current study (Bennet, 2001). Common for case studies is that they try to understand a specific person, society, institution or societal change and do this by assembling data, either qualitatively or quantitatively (or both), about the relevant object (Schrank, 2006a). Furthermore, case studies are often based on a wide variety of data sources and types, such as interviews, documents and surveys, which all need to be analysed in different ways (Schrank, 2006b; Eisenhardt, 1989). These various types of data sources enable *triangulation*, where multiple sources of evidence are used to gain an understanding of the phenomenon (Gerring, 2007). By using multiple sources of evidence, as well as multiple source types (data gathering methods), the results of the case study can be verified to a higher degree, reduce the bias of singular interviewees and increase the reliability of the empirical data (Vissak, 2010; Orum 2001).

Specifically interviews are among the most important data sources in a case study, because of the direct interaction and follow-up that is possible, so the researcher can guide the dialog in the desired direction (Yin, 2014). The interview can vary in how precisely it is planned, ranging from unstructured to completely structured, with the middle ground being semi-structured interviews. The semi-structured interview uses an interview guide just as a structured one but allows for some flexibility of the order of questions and follow-up questions (Bailey, 2007). During interviews, the aim is to ask questions in an unbiased and sometimes naive way, to create an environment where the interviewee isn't altering the answer because of being affected by the question (Yin, 2014). One example of this is to avoid the use of the word "why?" in a question, since it can make the informant answer in a defensive way, compared to using "how?" (Becker, 1998 p.58-60; Bailey 2007). The phrasing of a question can often affect the answer, and the questions should therefore be carefully formulated. For this reason the question "why?" has been avoided in the interview guides and appropriately replaced with how.

Whether a case study is appropriate for a research project depends on how the research question(s) are formed, and where the specific interest lies within the researched phenomenon. For a case study to be relevant the questions "how" and "why" should be prominent in the purpose of the study (Yin, 2014; Vissak, 2010). For this study these questions are very applicable since the interest lies in e.g.: *how* the city has approached the smart city strategy and *how* the tracking is configured.

2.1. Why Copenhagen?

When choosing a case the access to sufficient data is crucial, whether it be documents, interviewees or field observations (Yin, 2014). Therefore, the case that has the highest amount of available data should be chosen, although this might not always be known in the planning stage of a study. The geographical location of Copenhagen facilitates on-site observations and interviews for this study, as this thesis is conducted from Lund, Sweden. The second reason for choosing Copenhagen is that the city strategists and planners have, judging by international awards and indexes, been successful in making the city more sustainable and greener. Copenhagen is often called one of the world's greenest, smartest capitals and has been appointed "European Green City Capital" of 2014 (European Commission, 2014). Regarding the academic verdict of Copenhagen's sustainable and smart performance, the city's development of mobility by bike has been praised (Low, 2005). For further details on Copenhagen see the introduction of the city in Chapter 5. Thanks to Copenhagen's status as a sustainable city, one can say that it acts as a source of inspiration and incentive for other cities interested in sustainability, and study the solutions used in Copenhagen to form their own. Because of this the measures and solutions taken in Copenhagen might be of larger scientific interest than those taken in less "successful" cities.

2.2. Material Use & Data Collection

To facilitate triangulation, the case study is based on interviews, municipal documents, and field observations during a number of visits to Copenhagen. The interviews have been conducted with personnel from the municipality to gain an understanding of the nature of their Smart city strategy and how the Wi-Fi-tracking works. All interviews have been semi-structured, and interview guides are presented in Appendix 1.

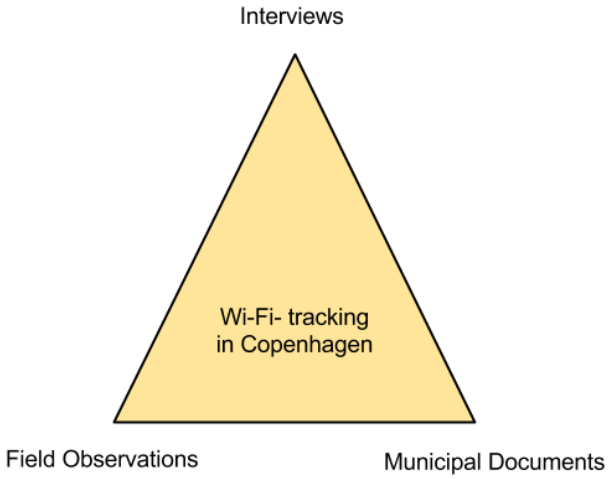


Figure 1. The triangulation of the different data collecting methods.

The municipal documents that are being used are official and have been published online, such as the CPH 2025 climate plan or municipal budgets. Their availability online assures that the municipality stands by the contents of the documents and that they haven't been withdrawn. Complementary to the documents, municipal web pages have been used to get the whole picture of the city planning. Web pages can sometimes offer more updated information than published documents, but as always with the internet, you have to be vigilant of the reliability of the information.

While the interviews and the document study are perhaps the most important data collection methods of this study, field observations are used to further deepen the understanding of the relevant phenomenon. The field observations, which are restricted to the streets where the Wi-Fi tracking is being tested, has one primary purpose. It will be used to gain an understanding of how evident and obvious the data collection is, i.e. if there are any signs indicating that the data collection is happening, or anything else that might notify citizens of the project. Overall the focus of the field observations will solely lie on the area and what data it can offer to the research questions that supplement the interviews and document study.

In addition to triangulation, another method model has been used to manufacture the case study, here called *the fundamental questions of the case study*. The mission here is not to change the way a case study is constructed according to classic methodology, but rather to illustrate it in a different fashion and for it to act as a thought model. The model, which is presented in figure 2, is based on the fact that "how?" and "why?" are the foundational questions, as written before, and therefore are the foundations of the model. They are analytical in their form and require significant empirical information to answer, compared to the four supplementing

questions of “What?”, “Who?”, “When?” and “Where?”. These are less analytical in their nature, require less information, and can be assumed to be necessary to answer the two foundational questions. Together they form the fundamental questions that are needed to investigate a particular phenomenon. Using this model, any missing case study information can be easily identified by considering what empirical information answers what question, and whether any question remains unanswered.

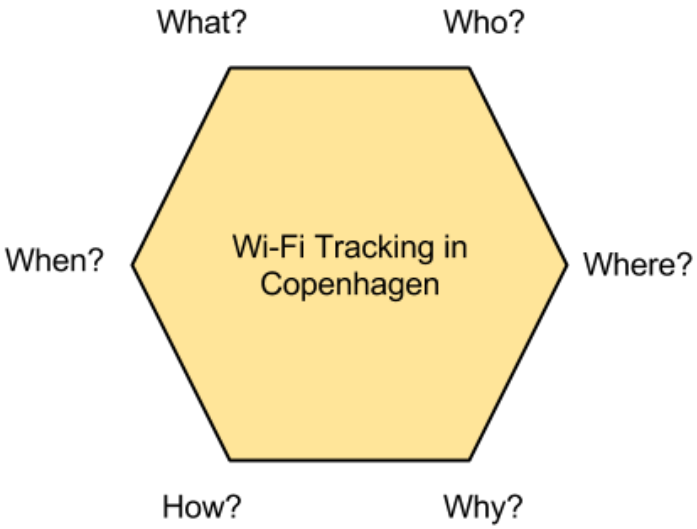


Figure 2. The fundamental questions of the case study.

2.3. Informants

The informants for this study have been chosen to include perspectives that are different and that will give a wider picture of the studied subject. The informants from the municipality have been Kim Spiegelberg Stelzer, a senior Smart city advisor for the city of Copenhagen, Søren Kvist, active in the structure of Copenhagen Connecting and Copenhagen Solutions Lab and Jos Bo van Vlerken, academic assistant at the Technical and Environmental Administration. To obtain an academic perspective these additional informants were interviewed: William Jensen[1], PhD fellow at a major Danish university and Stephan J. Engberg, internet security entrepreneur and EU researcher. A political perspective was provided by Morten Kabell, Mayor of the Technical and Environmental administration, was included, and finally to get a view ‘close to the citizens’ Magnus Boye was interviewed, a journalist from the Version2 magazine.

[1] William Jensen is an alias for an informant who wished to be anonymous.

2.4. Research Boundaries

This thesis is limited to one case of a city tracking citizens for sustainability purposes, and will not cover monitoring for security or criminality-decreasing reasons. Since surveillance for security reasons is a common phenomenon in modern cities, much research has been conducted in this area. Monitoring for sustainability purposes is on the other hand much less researched, especially when combined with a critical view on contemporary data collecting.

3. From Sustainable to Smart

The concept of sustainability surfaced during the 1970s and 80s, through literature like "Limits to Growth" (Meadows et al, 1972) and "Our Common Future" (WCED, 1987), where the latter defined sustainable development as meeting the needs of the present generation without compromising the ability of future generations to meet their own (WCED, 1987). Since then, many cities across the globe have invested much time and work to increase their sustainable and green qualities. And to do this, there must be a balance, equity and integration of work put into the three pillars of sustainability – environmental, social and economic development (Gibson, 2006). However, since the creation of sustainable development as a concept, it has been the target of considerable critique, often aimed at the flexibility of its meaning and the lack of practical applicability (Campbell, 1996). The idea of sustainability as being grounded in development by growth has made some scientists see it as an oxymoron and contradictory (Hornborg, 2001; Redclift, 2002). Also, the nonspecific character can create difficulties of measuring success, as the selection of indicators is up to the 'user'. Although these faults are serious and can problematize the use of the concept, they might be more directed towards urban futures and strategies in general than specifically sustainable development.

The Smart city is a phrase that emerged in the beginning of the 1990s as an indication of how urban development was shifting its focus to technology, innovation and globalization (Schaffers et al 2011). Since then it has become a very popular "urban labelling" phenomenon among cities (Hollands 2008). Despite the hype connected to the concept at this moment, the definition of it is fuzzy and sometimes inconsistent (Nam & Pardo 2011). The obvious characterizing ingredient of the smart city is the use of technology. In the smart city, all structures, for example power, water and mobility are designed, constructed and maintained using advanced technology, such as networks, sensors and electronics for the purpose of collecting databases, tracking and decision-making (Bowerman et al 2000). This is said to make the city safe, secure, environmentally sound and efficient. The traditional industrial cities of the 20th century are sometimes imaged as skeleton and skin while the post-industrial as living organisms with an artificial nervous system that enable them to respond to changes and coordinate the different parts of itself (Nam & Pardo 2011, Mitchell 2006). In the long term a smart city system will be able to monitor its own condition and perform self-repair, if needed (Bowerman et al 2000). Technology will be used as a balancing "ecosystem". While being highly technological and mechanized, a smart city can also give inspiration, share culture and knowledge with its citizens, giving them a motivating environment (Rios 2008). The

information and communication technologies (ICT) have a possibility of strengthening the freedom of speech and the accessibility to public information and services (Partridge 2004). One prominent feature of the smart city is *big data*: which is the increased amount of collected information via technology (such as sensors, networks and electronics) made to be compared and analysed (Boyd & Crawford, 2012). Open data is then the idea that these statistics should be available to everyone, including private citizens. Another aspect of the smart city is that the urban development often is entrepreneurial and business-led, and an opportunity for businesses to harness the societal changes (Caragliu et al 2011). This business aspect can be said to be rather logical because of the large focus on contemporary technology. Overall, the smart city rests on the integration of science and technology through information systems (Bowerman et al 2000). A more operational definition of a smart city is when: "investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance." (Caragliu et al 2011, p. 50). As pointed out at the end of this definition, the smart city must be able to involve citizens and actors in the change process. Lastly, when analysing smart (or sustainable or green) cities around the world an index is often used, with different categories and indicators. Several of these smart city indexes include a large variety of indicators of everything from greenhouse gas emissions to the amount of available iPhone apps that are based on open data. This modern use of the smart city concept can be compared to a buffet, where you can pick and choose what you want and don't want to include into the concept, and there is a large selection of things to choose among.

A more critical aspect of the big data and smart city debate revolves around the collecting and gathering of information that is private to the individual or that can harm the individuals' integrity. One issue is the pure amount of data that can be collected, which can be hard to control and manage as technology keeps evolving. When the focus isn't on collecting the data that's necessary or relevant, but rather on what *can* be collected — the limits of data collection are diminishing. Moving on, Martinez-Balleste et al (2013) showed that an increased collection of data on citizens could endanger their privacy and thereby decrease their freedom, and demonstrated how this happens with several smart city solutions such as location-based services (data based on the location of something or someone) and smart parking. The challenge for big data of not violating the privacy and integrity of individuals is therefore indeed very real and worthy of study. In many ways, managing big data is about stopping it from becoming big

surveillance — or any surveillance for that matter. And to do this, we must study the theories that try to describe, categorize and explain surveillance.

4. Theories of Surveillance & Monitoring

This chapter will go through some theories of surveillance that can be used when analysing a tracking or monitoring system, and offer a greater in-depth understanding of surveillance structures. The theories will then be used to analyse the case of Copenhagen in the upcoming chapter.

4.1. Orwell's Surveillance Dystopia

Arguably, the most well-known narrative on surveillance is George Orwell's novel, *Nineteen Eighty-four*, a dystopian big-brother story of an undesirable future society where electronic media and propaganda is used to monitor, influence and keep citizens under control (1949). A few pages into the novel the surveillance is described as:

> "Any sound that Winston (the main character) made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment." (Orwell, 1949 p. 3).

Firstly, the technology used to monitor citizens in Oceania (a fictional nation in the novel) is informational technology, such as the 'telescreen', a device that can be described as a combined TV and security camera (Orwell, 1949). Secondly, the surveillance portrayed is unknown in specific time, and makes the individual unsure of when the surveillance is actually taking place, an attribute that will be revisited in Bentham's panopticon. This characteristic is aptly put in the following sentences: "It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live — did live, from habit that became instinct -- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized" (Orwell, 1949 p. 3). Orwell's dystopia can, however, be called lacking in its modern technological applicability, which is understandable for an older novel, and one example of that is that the originator of the surveillance is the state — compared to the modern surveillance challenges connected to consumerism and corporate data collection (Lyon, 1994). Regarding the social controlling functions of surveillance, *Nineteen Eighty-four*, can however still be relevant.

4.2. Bentham's Panopticon & Foucault's Panopticism

Another theory of surveillance is Bentham's *Panopticon* that later was made more widespread by the works of Michel Foucault. Bentham designed a semi-circular building that he called

panopticon and it was meant to offer ideal rehabilitation and discipline by the setup of technology which intends to monitor, measure and correct the abnormal (Foucault, 1975). While the building was first and foremost designed to be a prison and the abnormal being criminality and violence, Bentham also saw the structure as appropriate for schools and factories to increase discipline and productivity (Bentham, 1791). Since it was more or less impossible to monitor a specific person constantly with the then available technology, the idea behind panopticon was to make sure that the person surveilled doesn't know precisely when the surveillance is happening, just that it always is possible. The person therefore assumes that the surveillance is constant (Bentham, 2002). This idea meant that the use of violence to promote good behaviour, whatever good behaviour might mean, was rendered unnecessary (Foucault, 1975). For this reason it is said that the surveillance should be known (either visible or in another way apparent and communicated) and uncontrollable (the individual doesn't know exactly when the surveillance is happening). Panopticon makes the surveillance permanent although the act itself isn't constant. The surveillance should, however, be maximized to the extent possible (Bentham, 2002). In the ring-shaped outer building, the cells of the inmates were designed to be completely visible from a centrally located tower in which the guards were stationed, making the inmates visible for the guards and the guards invisible for the inmates. This structural apparatus creates a system of inmates that are maintaining their surveillance and power relationships themselves, independent of those controlling it (Foucault, 2003). Thus the surveillance power becomes mechanized, de-individualized and disembodied.

Panopticon also has a scientific purpose — to determine and demonstrate differences between individuals since they easily can be monitored and compared without interference from others than just the individual (and the fact that the individual has knowledge of the surveillance) (Foucault, 2003). By doing this panopticon can be used as a science (power) laboratory where behavioural patterns can be corrected, since the activity in the different cells is highly controlled and there’s an abundance of information and data on the individuals (somewhat of a panopticon equivalent of big data). The structure makes it possible to intervene at any time and the constant pressure operates and adjust the behaviour before the fault has been committed (Foucault, 2003).

Another aspect of panopticon is that the building and activity should be established in such a way that makes it easy for anyone to understand how the surveillance works and grasp the information that is produced, i.e. a high accessibility of data (Foucault, 2003). In addition to this, the establishment should not only continuously be inspected by professionals but also by

the general public; a high transparency towards the general public is said to decrease the risk of power abuse and create a democratic and open surveillance process, which lets the exercise of power be controlled by the entire society (Foucault, 2003).

The size of the panopticon is in Bentham's depiction a limiting factor, since the glass construction in the cells needs a high level of light throughput and cannot be too deep (2002), but was described by Foucault as something that can be "spread throughout the social body without losing any of its properties...a network of mechanisms that would be everywhere and always alert, running through society without interruption in space or time" (Foucault, 1977 p.207, 209). This two-parted representation of panopticon as a concept can be ascribed to Bentham's focus on the physical establishment and the intrinsic functions it holds, while Foucault saw panopticon as a functional and structural apparatus that can be used to improve the exercise of power in society, called *panopticism* (Foucault, 2003).

4.3. Information Panopticon and Beyond

While the Bentham's panopticon was mostly focused on criminals and the disobedient, and Foucault's the disciplinary functions it could bring society, there have been attempts at using the theory of panopticon in other areas. In the book "In the Age of the Smart Machine" by Shoshana Zuboff (1988), she connects panopticon and technology with the workplace, and describes another type of panopticon. The *Information panopticon* doesn't need the structural apparatus that Bentham designed, nor the direct human supervision, instead it relies on information and communication systems that "translate, record and display human behavior" with the highest transparency and illumination for observational and controlling purposes (Zuboff, 1988 p.322, 332). Unlike Bentham's panopticon where the hierarchical structure is very obvious and solid, the informational panopticon has a more open and borderless hierarchy. At the workplace it may still be obvious who the workers and the managers are (i.e. the inmate and the guard) however, Zuboff showed that the surveillance works on a more horizontal level, called horizontal visibility and that the hierarchical surveillance roles become more interchangeable and drifting (Zuboff, 1988). Since everyone has access to the surveillance technology in the informational panopticon, anyone can act both as a guard and an inmate, a characteristic called surveillance collectivism (Zuboff, 1988). This is comparable to the idea of *sousveillance*, i.e. 'watching from bellow' or 'watching the watcher' (Mann & Ferenbok, 2013).

The concept of an expanded panopticon with modern capabilities was further discussed by Manuel DeLanda in "War in the Age of Intelligent Machines" (1991), where he compares

Bentham's panopticon with what he calls *panspectron*, using the example of the surveillance initiatives of the NSA. He explains the differences as:

> "Instead of positioning some human bodies around a central sensor, a multiplicity of sensors is deployed around all bodies: its antenna farms, spy satellites and cable−traffic intercepts feed into its computers all the information that can be gathered. This is then processed through a series of "filters" or keyword watch lists. The Panspectron does not merely select certain bodies and certain (visual) data about them. Rather, it compiles information about all at the same time, using computers to select the segments of data relevant to its surveillance tasks" (DeLanda, 1991 p.206).

Panspectric surveillance, *panspectrism*, have since then been further developed by Kullenberg & Palmås (2009), and comparisons has been made to the increased surveillance focus by European and US governments after the 9/11 terrorist attacks (Kullenberg, 2009).

In "The Googlization of Everything" by Siva Vaidhyanathan (2011), an important difference between the classic panoptic structure and modern digital mass-surveillance is identified, namely that the latter doesn't inhibit behaviour or change the way people behave. This is ascribed to the limited visibility and knowledge of the surveillance system to the average individual, in what Vaidhyanathan calls *cryptopticon*:

> "Unlike Bentham's prisoners, we don't know all the ways in which we are being watched or profiled – we simply know that we are. And we don't regulate our behaviour under the gaze of surveillance: instead, we don't seem to care" (Vaidhyanathan, 2011 p. 112).

4.4. Operationalizing Surveillance Theory

Based on the theories that have been presented, operationalization is used to create a more practical framework of surveillance that can be used in the case analysis of Copenhagen. This is done by identifying the most important characteristics of the surveillance theories and formulating a list of these features. This list is presented in table 1.

Table 1. Displays the operationalized surveillance characteristics, its respective theoretic origin and a description of it.

Surveillance Characteristic	Origin	Description
Known to the individual	Bentham's panopticon	Making the surveillance known to the person that's monitored is the first half of Bentham's surveillance principle of creating a structure where the monitored are maintaining their surveillance relationships themselves.
Unknown in specific time	Bentham's panopticon, Orwell	The second half is to make sure that the individual doesn't know when the surveillance is happening, which creates an illusion of a constant surveillance.
Uncontrollable by the individual	All	This describes the inability of the individual to choose when or what data will be collected. The opposite of this would be voluntary or self-administered surveillance.
Mechanized and Automated	Informational panopticon & Panspectrism	A trait of the electronically advanced surveillance system, which means that there's no need of human supervision (contrary to Bentham's concept) for the monitoring to continue constantly.
Geographically Centralized or De-centralized	Bentham's Panopticon and Panspectrism	The idea behind Bentham's panopticon revolves around a centrally located tower from where the surveillance is being conducted and administered, making the surveillance system geographically centralized. In Panspectrism, the surveillance technologies are spread much wider across the area meant to be monitored, in other words — the surveillance is not performed in the centralized area.
An aim (ambition) of being transparent	Bentham's Panopticon	A high accessibility and transparency of data for anyone interested means that the data collected can be easily accessed, understood and used by laymen.
Scalable	Panopticism and Panspectrism	Foucault's panopticism is described as something that can spread among society without losing any of its characteristics, which Panspectrism can be said to be a form of.
Collectivistic and non-hierarchical	Informational panopticon	A borderless hierarchy structure establishes horizontal visibility, making surveillance possible in any direction. This requires a transparency of data, which is described in a previous characteristic.
Non-specific in its data-gathering	Panspectrism and informational panopticon	One of the core features of Panspectrism is that as much data that can be collected should be, which then can be filtered for the relevant and desired information.
Directed towards controlling and adjusting the disobedient	Panopticon, Panopticism and Informational panopticon	The root of this characteristic is what purpose and function the surveillance has in a specific scenario. Bentham had "disobedience management" in mind, while Foucault had the discipline of society in mind. The informational panopticon has the purpose of observing and controlling human behaviour, much like the disobedience management of the two earlier. Panspectrism doesn't have the same specific nature of its purpose as the others, but can, thanks to its broad data-collecting, instead be used for many purposes. In this way, panspectrism is more uncoloured in its purpose than the others. Cryptopticon, on the other hand, doesn't want to change human behaviour like in Bentham and Foucault's models, but instead just gain as much information of a person's life and behaviour as possible.

5. Results – Copenhagen

This chapter will go through the findings of the study, divided into an introduction to the case (5.1), a more descriptive image of the Wi-Fi and Bluetooth tracking system of Copenhagen (5.2) and lastly an analysis of the empirical material (5.3).

5.1. Introduction to the City

Often called the capital of the Öresund region, Copenhagen aims to be carbon neutral by 2025, as proposed in the document *CPH 2025 Climate Plan* (2012a). Apart from a reduction of CO_2-emissions, the city continues its efforts of improving cycling mobility, increasing green electricity production and planning a green and blue urban area that has environmental, economic and social benefits (2012b). One of the main initiatives of the Climate Plan regarding energy consumption is that "Copenhagen must be developed into a *smart* city. A digital infrastructure must be laid down for public data for electricity and heat consumption" (2012a p.10). In conjunction with this, Copenhagen received funds for two projects in 2011 (to 2015) as a part of EU Smart Cities (Copenhagen, 2013a), with different areas of focus within the smart city. The first of these deals with "Planning for energy efficient cities" (PLEEC), which aims to connect scientific knowledge with innovative private companies and ambitious cities to reduce energy use (EU-Smart Cities 2014a). The second aims to make integration a more crucial factor in the smart city, by "including strong stakeholder involvement, data analytics and smart tooling, financial strategies and methodologies for co-creation, like service design thinking." (EU-Smart Cities 2014b). Aside from these two projects, Copenhagen has also made three commitments as a part of EU-Smart Cities, two of which concern smart energy and transportation, and the third citizen participation with a highlight on gender and diversity mainstreaming (results expected in 2014-2016 and beyond) (EU-Smart Cities, 2014c,d,e). In 2013 Copenhagen was awarded the IBM Smarter Cities Challenge Grant[2], with aspirations of addressing how management of data can help the city to reach its goal for 2025 (IBM, 2013). Some of the resulting recommendations were to integrate key stakeholders more effectively, to address the lack of standardized data among data producers and consumers, to focus on driving innovative ideas in conjunction with the 2025 goals and to engage the public participation with a structured approach (ibid). The report also concluded that there is a "lack of data and lack of

[2] IBM's Smarter Cities Challenge was initiated in 2011 and consists of a group of IBM experts that interview stakeholders in the chosen city and then deliver recommendations to the city leadership on smart improvements (IBM, 2013).

access to monitor pedestrian flow, traffic congestion, traffic prediction and weather impacts" (IBM, 2013 p. 8).

5.1.1. Copenhagen Connecting

Established in 2013, Copenhagen Connecting (CC) is the city's initiative on digitizing the infrastructure by the use of big and open data, a big step in the direction of the smart city.

> "The municipality of Copenhagen aims to establish a digital infrastructure that covers the entire city and serves as the main road for Copenhagen's large amounts of data. The concept is called Copenhagen Connecting and makes Copenhagen an international leader in green growth through innovative technology solutions[3]."(Copenhagen, 2013b p. 1).

This is done by creating a city grid of both wireless and fibre-optic networks which are then connected to an open data portal[4] where public data can be found, such as parking spaces and current traffic activity (Copenhagen Connecting, 2013a). The initiative's goals encompass to work with:

- targeted use of data in solving problems
- new technology or known technology in new ways
- efficient use of the Municipality's or City's resources
- new ways of involving citizens (ibid)

It is clarified that the Copenhagen Smart City aims to break down technological and organizational silos that can be created when organizing work in a structured way, to further facilitate a smart development (Copenhagen Connecting, 2013a). CC enables four core services, which all involve digital infrastructure and the first being; asset tracking. By using Radio Frequency Identification (RFID) tags, the tracking of items and equipment is made possible and can be used to reduce theft of bikes and cars. Secondly, the sensor platform collects data on the city conditions which can be used for real time monitoring of e.g. CO2-emissions, waste collection and sewer conditions. The third is cost-efficient data connections, where the city grid can be used for the existing infrastructure (unifying data communication) such as traffic lights and charging stations, as well as making the Wi-Fi available for all citizens and tourists (Copenhagen, 2013b). The last one, Big data city flow is the most relevant out of the four for this study, and it is the data collection from "triangulated Wi-Fi devices (that) creates knowledge about people's movements, cars, bikes etc. throughout the city in real time and

[3] Own translation.
[4] http://www.data.kk.dk/

aggregated over time" (Copenhagen Connecting, 2013a p.5). To exemplify this in a practical form, it can according to CC be used to optimize traffic flow, increase knowledge of traffic jams and find solutions to congestions (Copenhagen, 2013b). It can be used for crowd control during public events as well as the efficient routing of emergency transports through the city (Copenhagen Connecting, 2013a). Additional purposes are pricing parking spaces based on the local traffic situation or the availability of parking spaces in the area.

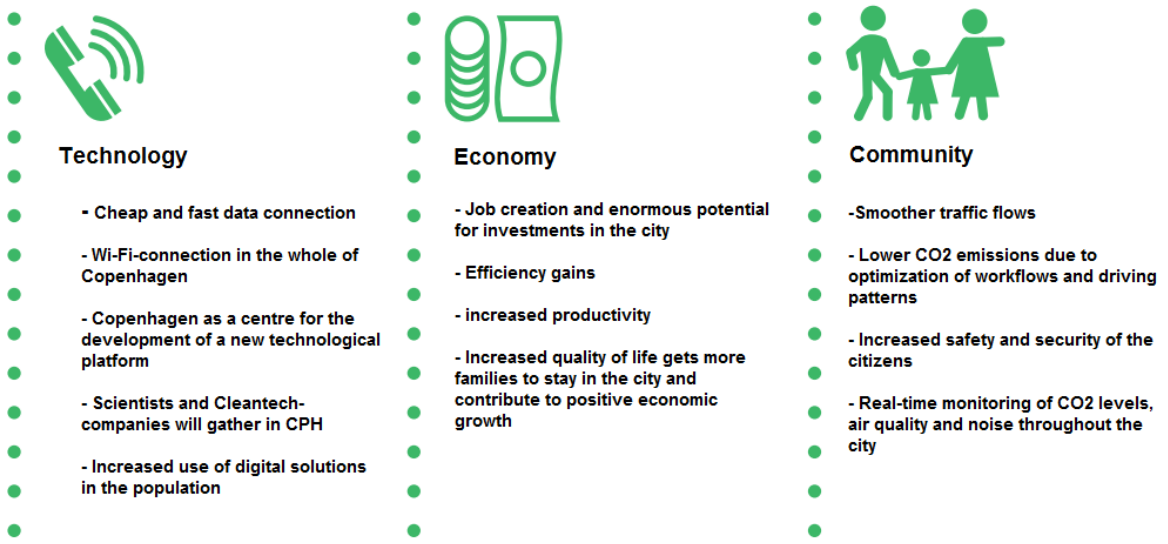


Figure 3. Own translation of the benefits of Copenhagen Connecting according to the Copenhagen Municipality. The original figure can be seen in Copenhagen (2013b, p.2).

5.1.2. Partnered Actors

Because of the large infrastructural changes[5] that Copenhagen Connecting proposes, and the integration that such a system demand, CC must itself also be well connected and integrated with key actors. These connections can facilitate and speed up the establishment of a digital infrastructure, as well as developing the technologies and concepts that can be used within the system. One of these actors is Ramböll, the Danish consulting firm, which has conducted a pre-feasibility analysis on CC with the aim of studying the economic value of the solutions and changes that CC propose. After dividing the analysis into three areas; Infrastructure and Environment, People and Organisation, the following is said of the analysis of the peoples' situation:

> "A wireless and wired network like CC has not previously been implemented on such a large scale, so it will be of great significance for citizens, businesses and tourists in Copenhagen. CC will affect many types of people, for example by ensuring that patients

[5] Although the physical infrastructural changes might not be vast, the digital infrastructure requires large investments in devices that allow for the data communications to be possible, thus the (digital) infrastructural changes can be called large.

> can more easily be connected to tele-health solutions, vulnerable citizens can be helped with tracking devices and large crowds can be better guided through the city. Furthermore, CC help to provide tourists a better experience of Copenhagen. Tourists will experience gains in the form of free WiFi, and the digital infrastructure novelty will help to attract more tourists[6]." (Ramböll, 2013 p. 1)

The report goes on to present the monetary results of the feasibility analysis, including avoidance of traffic jams, energy optimization, effective crowd control and so on, with the total economic gains mounting up to 4,4 billion d.kr. (Ramböll, 2013). A considerable chunk of this, 1.7 billion, is also said to be annual profits. Although the document does account for the risks and barriers that they could identify when implementing a digital infrastructure, these are more directed towards technological issues such as the unreliability of a specific technology, than the risk of undermining the integrity and privacy of citizens. On the contrary, the digital infrastructure is said to enhance the security of citizens, predominantly elderly[7] and children (Ramböll, 2013 p. 77). Specifically on the topic of data collecting from citizens it is said that: "by using big data vast amounts of data can be collected on the use of the city, its functions and more. It is expected that this data can be used for optimization, development and resale to private companies and research institutions, etc. (...) thereby, it is expected to create new opportunities for growth for the city of Copenhagen" (Ramböll, 2013 p.7).

Copenhagen Connecting has also made connections with several universities[8], that have all have given expert advice regarding the plans and ideas associated with CC (Copenhagen Connecting, 2013b) but although these statements might have improved the plans and strategies of CC, none of them mention privacy or surveillance risks with the project. Apart from previously mentioned Ramböll, some of the other private businesses that have some sort of partnership with CC are Blip systems, Hitachi, Alexandra Instituttet, Gartner, Kraks Fond, Confederation of Danish Industry, Cisco, Silver Spring, Citelum, Leapcraft and Copenhagen Capacity.

5.1.3. Open Data platform

As well as investing in big data (using the data collection methods described before), CC aims to create a transparency in the digital infrastructure, by the use of open data. Initiated in 2013,

[6] Own translation.
[7] According to the report, large gains can be made from communicating with elderly when they are still in their homes and thus saving some of the labor costs (Ramböll, 2013 p. 76).
[8] Technical University of Denmark (DTU), University of Copenhagen, IT University of Copenhagen and Aalborg University.

the Copenhagen Open Data platform is designed to open up the use and availability of data from the municipality systems and is anchored in the Technical and Environmental administration of Copenhagen (Copenhagen, 2015). Although still in beta, it serves as a 'lighthouse project' for Smart City Copenhagen, where diverse types of data share room, such as: parking spaces for cars and bikes and municipal parking meters. At the moment, the platform only contains limited amounts of municipal data, but the desire is to create "bridge between public and private data, so data sets from many different actors can be linked together in new and exciting solutions (...) to ensure that both public and private data can come into play as the future growth engine." (Copenhagen, 2015).

5.1.4. Previous Study on Copenhagen Connecting

Preceding this study, the subject of Copenhagen's smart city has been investigated in Liv Holm Carlsen's "The Location of Privacy- A Case Study of Copenhagen Connecting's Smart City". Published in August of 2014, the study takes a case study approach and examines what privacy implications the project of Copenhagen Connecting has, and does this with a theoretical foundation in privacy and the smart city. Although Copenhagen Connecting was commenced in 2013, the first actual measures that the initiative took were the demonstrations that were planned to start in the fall of 2014. The EU did not fund the demonstration that fall, and it was therefore postponed to 2020 (Kvist, 2015). So, this means that Holm Carlsen's study doesn't look at the concrete consequences of the initiative but rather the plans of the project, supplemented with an interview with the head of Copenhagen Connecting Søren Kvist. Despite this, the previous study can give a good foundation on the dangers of the smart city to coming studies such as this. Based on the studies of Andrejevic (2007), Gordon & Souza e Silva (2011), and Albrecht & McIntyre (2005), Holm Carlsen writes that RFID tagging of private things could give the municipality the ability of digitally monitoring the inhabitants of the city, without the person's knowledge or control (2014, p.43). The issue then becomes if the individual can trust the municipality (and its private affiliates) with this personal data and its uncertain subsequent uses. One can also argue that the individuals' trust of the municipality loses its meaning and necessity when there's no alternative to getting your personal data collected. Holm Carlsen also expresses some scepticism on Copenhagen Connecting's use of life quality as a positive gain of the initiative and in what way the digital infrastructure will increase the life quality of the citizens, and argues that control of personal data, as well as trust in the municipality might be more fitting indicators in this case (2014, p.45). Interestingly, Holm

Carlsen notes that she could not find any data or documents on citizen participation or involvement, though this might be due to the initial state of the project (2014, p. 24).

During Holm Carlsen's interview with Søren Kvist, he explained that the possible data uses of the collected data are not all known, and that this is one of the points behind big data — to make possible a potential of growth based on data (2014, p.58). On the topic of open data she writes that "creating a transparent city by the production of an open data portal fails miserably", as it might just be an illusion to give the impression of transparency (Holm Carlsen, 2014 p. 64).

5.1.5. An Update on Copenhagen Connecting

As described so far in this thesis, Copenhagen Connecting is designed as grand project for the digital infrastructure of Copenhagen, but this image seems to have changed since the publication of Holm Carlsen's study. During an interview with a Smart city senior advisor at the municipality it is explained that:

> "You could say Copenhagen Connecting started out two years ago, where we thought it would be a big project covering all of Copenhagen. If you build a digital infrastructure then we made some estimations and business cases…if you have this project fully implemented all over the city the socio-economic gain would be 4, 4 billion Dkr per year. But it also requires a lot of investments and you're not 100 % sure what you get…and the technology runs so fast so we couldn't make the politicians make this kind of investment, which I think is a very good idea. But now we work with Copenhagen Connecting, let's say as a vision that we try to work towards. But what we do very concrete now is that we take out the elements that we can find funding for, that are relevant and then we do these projects…and if you sum them all together you get closer and closer to the idea of Copenhagen Connecting. But with Copenhagen Connecting and open data we realized that we cannot just make one big model, invest a lot of money, you have the right model, and it will solve everything. So we found out that what we have to do is that we have to demonstrate, we have small solutions and we demonstrate them and if they work, then we scale them up for let's say a neighbourhood, and maybe for the whole city. So, that's the way we work now and that's also why we have established Copenhagen Solutions Lab with four persons, and they're also working across administrations and silos, the main task is to make partnerships with private companies, make solutions together with the private companies and other municipalities, universities and organisations. Because that's also one of our ideas with the smart city, that it's not the municipality alone who can do it, we have to work together with all these resources" (Spiegelberg Stelzer, 2015).

What this information tells us is that CC has gone from being a grand project that was aimed to be established as a whole, to a visionary concept that the municipality strives to reach. This shift in how the municipality sees Copenhagen Connecting could be reflecting some of the problems associated with a Wi-Fi and Bluetooth tracking system, which will be analysed further on in the study.

5.2. Wi-Fi Tracking in Copenhagen

The following segment will go through; the basics of Wi-Fi tracking, general privacy concerns with such a technology and the tracking system of Copenhagen.

5.2.1. How does Wi-Fi tracking Work?

To be able to track individuals in the city, several technologies can be used, such a GSP (Global system for mobile communications) but most usual today are Wi-Fi and Bluetooth. They are technologies used for short to medium range wireless communication and are today built into an array of devices like smartphones, tablets, laptops and cameras. Focusing on Wi-Fi, it often has a built-in encryption of the data that's being transmitted so its security is increased, although this depends on the particular encryption and the network provider. To get an internet connection the Wi-Fi device needs to be able to connect to an access point and does this by sending a signal with its MAC (Media Access Control) address, a global unique identifier for a specific device (Cunche et al, 2014). These signals that are emitted are not only sent when the device is connected to an access point but also at all other times, with the regularity partially depending on the physical environment (Abedi et al, 2013). In a study conducted by Cunche (2014) the regularity of this signal, *the probe request frames*, from two smartphones of Samsung and Apple are described as a typical period of 40 second for the apple device and 30 seconds for the Samsung. Another study, by Abedi et al (2013) looked at how long the MAC address discovery time is (the time for a sensor to get a devices' MAC address) and found that it was around 1 second for Wi-Fi devices and around 10 seconds for Bluetooth. Because of this high regularity and rate of the signal, and the large quantity of Wi-Fi devices that are found in the modern city, tracking MAC-addresses is a very effective way of tracking the mobility of cars, bicyclists and pedestrians (Ibid). This is done by triangulating Wi-Fi and Bluetooth sensors which measure the distance between the desired device and the sensors over time (Giannotti & Pedreschi, 2008).

5.2.2. General Privacy Concerns

As previously mentioned, while the data that's being sent over a Wi-Fi network can be encrypted (although with several faults), the MAC address is sent in plain text and is never

encrypted, which makes it very easy to intercept and collect (Cunche, 2014). Because the MAC address acts as a pseudonym for a person that's being tracked, and isn't directly linkable to a mobile number or a name, the collection of MAC-addresses is sometimes portrayed as privacy safe and secure, avoiding possible privacy infringements (Abedi, 2014). This has been proved false by several studies, with some of them being; Greenstein et al (2007), Pang et al (2007), Golle and Partridge (2009), Lindquist et al (2009) and Cunche et al (2014).

Greenstein et al (2007) showed that when a Wi-Fi device scans its environment for a network, some devices send out a signal with the SSIDs (Service Set Identifier) that the device previously has connected to, i.e. the names of the Wi-Fi networks that are prefered and previously used by the device. The SSIDs are sent out in plain text and unencrypted, allowing the device-owners' previous locations to be known, as SSIDs typically are unique. Greenstein et al writes: "he advertises where he *has been*; i.e., an attacker could use this technique to compromise a victim's *past* privacy" (2007). It is added that this technique is possible even with devices that change their MAC-address frequently or that only connect to encrypted access points.

Golle and Partridge (2009) later demonstrated that by knowing the daily travels of an unidentified person, from home to work, the threat of re-identification of a person substantially increases, than having just one of them. This is due to the unique locational qualities that the home-work combination has. Location can thus be a very powerful pseudo-identifier, as long as you have access to an anonymous person's home and work locations, which a MAC address tracking system has, as long the home-work area is covered by sensors. Even when removing the unique addresses and names Pang et al (2007) were able to track users; "although we found that our technique's ability to identify users is not uniform (...) most users can be accurately tracked. For example, the majority of users can be tracked with 90% accuracy". It is subsequently concluded that "pseudonyms are insufficient to provide location privacy for many users" and that "an adversary needs only 1 to 3 samples of users' traffic to track them successfully, on average." This means that a continuous tracking process makes the un-identification more and more successful, as the pseudo-identifiers get more data. Pedreshi et al adds:

> "Clearly, the removal of identity is not a fail-safe solution to identity protection, especially when quasi-identifiers are used as pseudonyms. Yet, even a brute force solution, such as the replacement of identifiers with unintelligible codes, may not be sufficient when the data to be disclosed correspond to mobile and geographic information, such as personal trajectories" (Pedreshi et al, 2008 p.104).

One of the ways of addressing the tracking issues with a MAC address is to hash it, a cryptographic function used to encrypt data, by creating a seemingly random combination of letters and numbers of some input data, in this case a MAC address. Such an encryption can however sometimes act as a false promise of security as several cases are known where MAC addresses were successfully un-hashed (Demir, 2013; Mayer, 2014). Demir concludes in his thesis "hashing a MAC address is not a satisfactory solution. Several methods more or less fast allow an adversary to discover the hidden MAC addresses" (Demir, 2013 p. 19).

All these issues, in combination with the tracking of MAC-addresses make privacy of identified citizens much in danger of an infringement and very much at risk of being personally tracked.

5.2.3. The Tracking System of Copenhagen

The Wi-Fi and Bluetooth tracking system was started on the 16th of June, 2014 and is a part of the intelligent traffic system (ITS) that Copenhagen has started. ITS is a program within the traffic department of the Environmental and Technical administration, and was established as a part of the CPH 2025 Climate plan. At the moment, eight sensors are installed in the central part of Copenhagen, across H.C. Andersen's Boulevard, more precisely showed in figure X (Van Verkel, 2015). Another nine sensors will be put up in the upcoming weeks to further increase the data collection. The field observations showed that the sensors are put up in four pairs where the lower one is assumed to be the Wi-Fi sensor and the higher one Bluetooth (pictures from the field observations can be seen in Appendix 2). On site observations also showed that there are no signs or no indication of a tracking system, meaning it's more or less impossible to know about the project when you walk in the affected area.

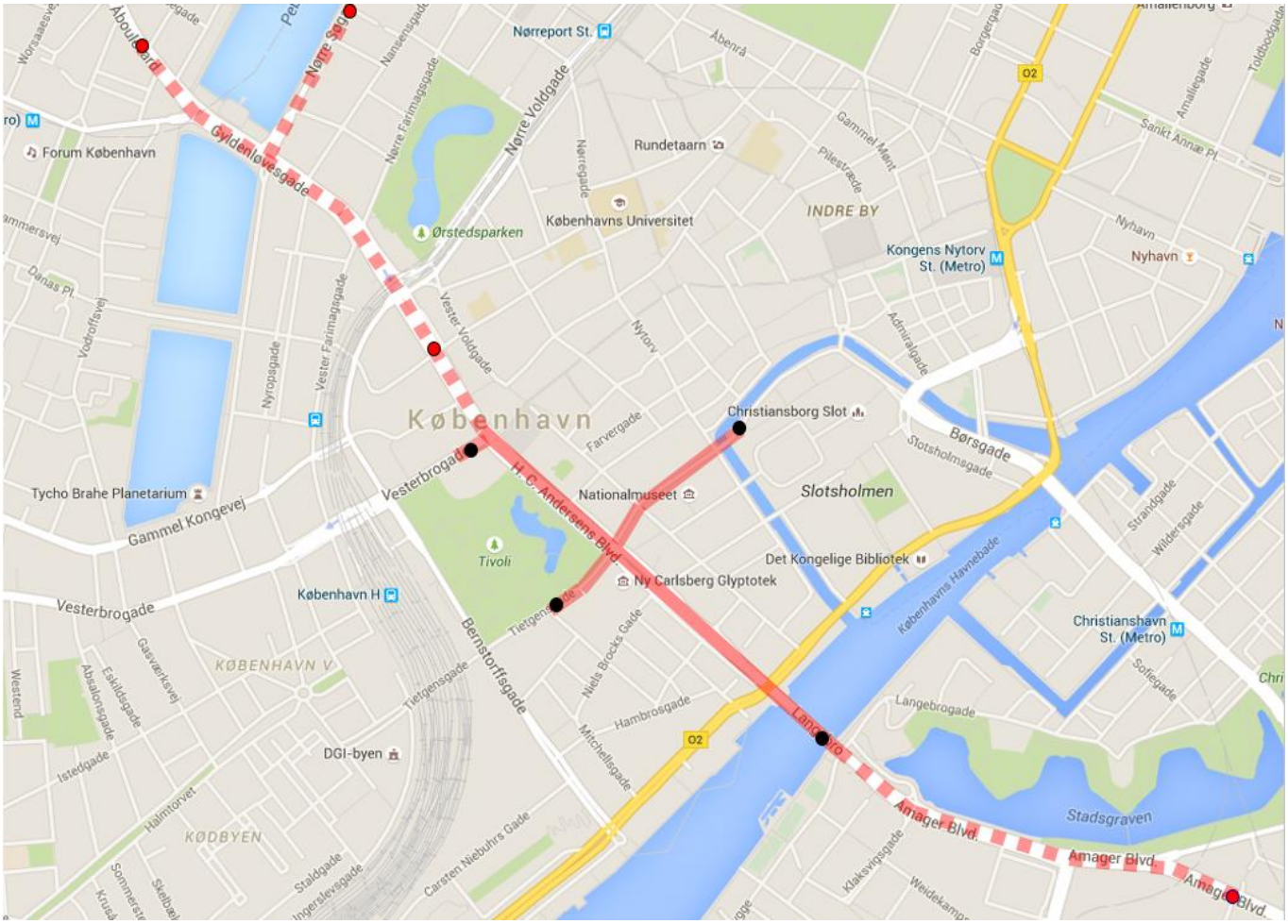


Figure 4. Marked in solid red is the Wi-Fi and Bluetooth tracking area and the 4 black dots show the location of the sensor pairs, based on field observations. The dotted red lines show the expansion of the project that is planned, vid sensor pairs marked in red.

The company that builds the sensors and handles the data collected is Blip Systems[9], and has an indirect relationship with the municipality of Copenhagen which is mediated through the consulting firm COWI. The product that is used is called the Bliptrack Wi-Fi and Bluetooth traffic sensor and works by collecting MAC-addresses as explained before. When the Bliptrack sensor detects a MAC-address it uses an algorithm to generate a hash code for the device and stores parts of these hash codes to follow devices around (Blip Systems, 2015b). The algorithm is changed every 24 hours in order to reduce the risk of identification on the basis of daily travel

[9] Blip Systems products are used in many Danish municipalities, and as well spread internationally. A representative from Blip Systems say that Copenhagen is just one of about 20 Danish cities that use their products. Some of the more successful clients has been various airports (e.g. Copenhagen Airport) using their products to predict queue time and airport management (Blip Systems, 2015a). Several other companies that offer a similar product are known and some of them are: Bumbee Labs, Navizon and Euclid Analytics.

routines. The system then uses cloud servers to store and process the hashed data, that for now only is accessible to the Copenhagen Municipality. There are plans on making aggregated versions of this data available to the public in the future. The system is reported to have cost the municipality 140,000 Dkk so far, with additional costs of 250,000 Dkk to expand the system (Boye, 2015c). Blip systems address privacy by stating: "The raw data from the sensors is encrypted and transferred to a secure cloud server, where it is extracted and separated" (Blip Systems 2015c). "BlipTrack ensures privacy by having the individual sensors convert the detected devices into anonymized and encrypted hashes. This fine-grained approach to privacy, allows local authorities to meet the requirements of the Data Protection Act" (Blip Systems, 2015d).

This project is being communicated through several documents, with varying specificity, and one of them is "8 New Intelligent Traffic Solutions", where the project is called "better flow on the streets" (Copenhagen, 2014). The document explains how the ITS system work, by triangulation of Wi-Fi sensors, and what the data can be used for in traffic planning scenarios. It's also explained that the solution was tested at the Technical University of Denmark, unfortunately not where this specific project will be established.

5.2.4. Ruling of the Danish Business Authority

In January of 2015, a chief manager from the Danish Business Authority[10] (DBA) said that the Blip Systems MAC-address collecting is violating EU regulation; "You may collect the MAC address if it is necessary to perform the service that the user requests. Should you additionally use it for other purposes, then you must ask for customer consent" (Boye, 2015a). He continues; "If it goes beyond what is necessary and what the user has requested, it is covered. And this is the case here. In such cases, the Directive requires that you obtain users' consent" (ibid). This verdict affected a lot of cities in Denmark utilizing the Bliptrack system, such as Aalborg and Aarhus, which generally seem to be assuming that the Bliptrack system is legal, and that it's the technology supplier that is responsible for law abiding (Boye, 2015b). Blip Systems themselves say that they want to comply with the relevant legislation, since they are selling their products in many countries, but they also say that it is the buyer of a product that has to ensure that the product isn't breaking any country-specific laws (Boye, 2015b). Moving on, they also say they have a function that allows individuals to control how long data is stored in the system.

[10] A state organization that tries to "create the best conditions for growth in Europe, and to make it easy and attractive to run a business in Denmark" (DBA, 2015).

Based on the statement of DBA, that citizens have to give their consent for the collecting to be legal, Copenhagen chose to pause the collection of MAC-addresses in February and await some clarifications from DBA (Boye, 2015c). According to the municipality's project leader for intelligent traffic management, they were awaiting feedback from the DBA, and had heard about the possibility of granting an exemption for these systems, so that they once again can be used (ibid). Copenhagen also stopped the expansion of the project at this point (Boye, personal interview, 2015).

In March of 2015, the DBA ruled that the Bliptrack data collecting system was not violating the EU privacy regulations, because it doesn't allow for the identification of the user. In their statement it is written that: "The authority has in the ruling put an emphasis on that the data collected is anonymized in a reassuring way. This is because the Authority believes that the collection falls outside of the rules intended to ensure users from interference with their privacy. The reason is that the rules must safeguard the protection of citizens' privacy, and that this safeguard is built into the solution" (DBA, 2015a). The DBA has in their ruling factored in that it's difficult for Blip Systems to communicate directly with the users, which they say make it impossible for Blip Systems to inform citizens and obtaining their consent (DBA, 2015b). They go on to say that: "DBA has also particularly emphasized that Bliptrack immediately hashes and encrypts the MAC addresses collected by the system, and that, then, even with the help of all reasonable aids, will not be possible to get back to the original MAC address. The algorithm by which the system hashes MAC addresses, is also replaced randomly after 24 hours, after which it will no longer be possible to monitor the anonymous MAC address as the hash value of the MAC address is no longer the same" (DBA, 2015 p. 4).

5.3. Analysis of the Case

For the next segment, a presentation of interview results and an analysis will be made of the Copenhagen case, divided into the following categories: Smart city, Wi-Fi tracking, citizen involvement, conflict of interests and privacy.

5.3.1. The Smart City Strategy

Firstly, the Smart city strategy can be approached in so many ways, and with different intentions, so mapping the way that Copenhagen uses the concept is a good place start. On how Copenhagen uses the strategy their senior Smart city advisor explains:

> "One thing that's very important to say is that some cities work very hard to become a smart city…we see it a bit different. We have our real goals, you can say, which is to create a better quality of life, to create a CO2 neutral city and to create growth, and all the work we

> do with smart city is more like a tool, a toolbox that we use for our real goals. It's not a goal in itself to be smart or to use all the technology that exists, we only use it when it makes sense to reach our real goals as a city, and that's always with the citizen in focus. So we always have to keep that in mind. We are often presented to some partners or some companies, whoever they are, they come up with some fantastic technological tool we always say "yes it's smart but maybe we don't need it and maybe we need something else instead". So it's very pragmatical, but I think a very healthy way to go, instead of some cities have bought huge systems or dashboards and maybe it doesn't really change so much. So we look very closely at the products and see what we really need and what can help us and make some prioritising" (Spiegelberg Stelzer, 2015).

This means that Copenhagen isn't working towards becoming a smart city per definition, but rather works by using it to reach their overall goals. Though, as stated before, the new application of Copenhagen Connecting is to work with it more like a vision than a specific project, meaning it more or less becomes a type of goal for the city, and it can be argued that such a step would need a political decision too. Whether the Smart City strategy is a result of a big decision it is said from the municipality's side:

> "We haven't had any political decisions so far on a smart city strategy…not a big one. It's politically decided that yes we should work with smart city and this direction, but it's not like it's a vision for Copenhagen that the politicians have decided. What might also be important for you to know is that the politicians decided to make a project council for smart city that works across all seven administrations…and they know about it and they work with it with this in the mind "ok, this is the kind of direction we want to go". And the project council is one director from each department…actually it's quite exceptional because there are only two themes that have project councils across all departments. This smart city project council is one of them and the other one is for citizen projects. So just to illustrate how important it is for the politicians and how much effort there is in this smart city to work across the silos. Because otherwise all the projects are mainly in all other administrations. But here we work across all seven silos" (Spiegelberg Stelzer, 2015).

So, the walk down the smart city path seems to be a politically decided one, although thanks to the nature of the smart city concept, a lot of flexibility is possible in what measures to actually choose. On one side the Smart City strategy is one of the themes that concern all seven departments, and on the other side it's not a vision that they've decided on politically. In contrast to this, William Jensen, currently a researcher in Denmark, shares view on how a smart city strategy can develop within a city:

> "Having spent some time in planning and seeing how things are in the real world, it's easy for people to be blinded by possibility and not see either the dark side of something or the unintended consequences. And I think in this particular area, and it's not just Copenhagen, it's most of these cities, they're buying a vision that's being sold by tech-companies without understanding the consequences of it. The existing tech-companies, IBM, SAP and Oracle and Hitachi, Accenture, the ones that are really pushing this agenda on Smart cities…their business is dying. IBM has missed their quarterlies every year, every quarter for the last four years´, Oracle's only hit their targets six out of twelve, SAP is in trouble…everybody is in trouble. It's because private businesses don't want to use their products anymore, because the free version is better. Cities don't know this. Municipalities don't know this. Regions don't know this. National governments don't know this. So I think for them, they're looking at this a very fat market, with very nice margins. And they sell this stuff (the Smart city) to the mayors, to the politicians, and then to the techs inside" (Jensen, 2015).

The weighing of the possible consequences and benefits of a specific measure is crucial to deciding whether to go through with the change, but naturally the choice depends on how it's weighed and what is seen as success or progress. The fact that possibility can be a blinding factor of unseen consequences, is an issue maybe more prominent than usual, when trying to come up with new innovative solutions in hope of addressing the urban challenges. Jensen goes on to address the recognition that Copenhagen has as a sustainable city:

> "I think Copenhagen is very good at marketing. I think there's some substance behind the marketing, but I also think that they're extremely good at selling the story. I'll give you an example: So, they're intended to be the first climate neutral capital by 2025. If you actually look behind the numbers, what they're actually going to do, in transport for example… they're not going to reduce actual emissions - they're going to buy offsets by planting forests someplace else in the world. That's one piece, the other piece is that in the switch from coal to wood pellets in the three combined heat power plants, the induary changes in land use that result from deforestation, there are direct results in the south-east of United States and in Siberia and Eastern Europe – it's actually 16 % more carbon intensive than coal. But what Copenhagen is doing is, they're putting up an invisible wall around the perimeter of the city and saying look: "we're not emitting any CO2". And there are a number of these paradoxes you can find. I think in the smart city stuff right now, this is the euphoric high. I don't know if you've seen Gartner, he has a very classic graph[11] of technological developments, I can't remember the exact terminology they use but it starts of as a little

[11] The figure referred to can be viewed at
http://blogs-images.forbes.com/gilpress/files/2014/09/gartner_2014-2.jpg

> idea, and then there's this great euphoria, so everything is great, it's going to change everything. And then on the backside…they call it the "trough of disillusionment", and I think we haven't reached the trough of disillusionment yet. I think we're still in the euphoric stage…because so much of this conversation is marketing talk. Marketing talk from the tech companies, the metal pushers and the hardware people to sell gear, to sell products and services to the cities. And the cities on the other hand, they tell themselves, internally and externally, how great they are and what they are doing, but the truth is when you see on the ground, when you look at what they've done, they couldn't tell you what the actual cost was, the actual benefit was, the projected cost and benefit, what went wrong, what went right, because there's no evaluation. Not systematically" (Jensen, 2015).

One can discuss how much a municipality should spend on marketing, but still, marketing the city will lead to greater interest among private businesses to invest in the city — as long as the marketing isn't misleading or inaccurate. The question is how this can affect the citizen, and the problem arises when the citizen is negatively affected by these privatively initiated projects. What the actual task of the municipality is in the smart transformation is not always clear, and is described by Copenhagen's senior Smart city advisor:

> "You could say that our main task as a municipality is to define the challenges…that we want the companies to look at. One example is…we've had some flooding in Copenhagen, where the water comes up in the street and for that we have a partnership with Cisco and some surrounding municipalities. And what we do is, we mainly define the challenge and then they come up with the solutions. But of course we are also developing the solutions in close cooperation. Right now we are applying for EU-funding for some projects and then we sit together with…for example we're making an intelligent urban street we call it, and there we define the problem and we set up the solutions together with the companies. Another big project that we're working on is something that we call the "climate-block", where we have selected a block (neighbourhood) of buildings where we want to make solutions with solar power, ventilation, energy savings and smart meters. And then we sit together with the companies, the specialists in this area and also with DTU (Danish technical University), for example, and we find out what kind of solutions can work here. So it's a combination" (Spiegelberg Stelzer, 2015).

So the city in this case uses external private actors in its city development to find relevant or suitable solutions, and as seen before tries to prioritize and choose those solutions that in the highest degree suit the challenge. This can be seen as a balancing scale of on one hand the ability to use local company innovation and on the other the risk of creating conflicts of interests

between the private company, the municipality and the citizens. Regarding the risk of conflicting interests Spiegelberg Stelzer adds:

> "Well, it's two different worlds and sometimes it's hard to cooperate, because sometimes we have a common goal…and sometimes it's difficult because private companies also have to make money, and sometimes it conflicts a bit when we want to demonstrate some things and these two don't go together. But having said that it's also true that Copenhagen is a place where a lot of companies come and want to test their ideas, because we're willing to go into testing and cooperating. For example we just made a partnership with Hitachi, who are making a platform for big data where we can basically put all our public data into it, and we provide that for free. You can put data from providers, like HOFOR, who provide electricity, and these companies, and also from private companies. And they should develop a platform where they can make it economically viable and make money out of it. And we give them some money to start developing this platform but they also invest a lot themselves…extra. And they do that because they say that if we can create a solution that works in Copenhagen and test it, then after that we can go and sell it worldwide, and maybe make a lot of money. And for us here in Copenhagen we're just happy as long as they make the solution in Copenhagen. So that's a partnership that I think is going to work very well, and we just started on that a few weeks ago" (Spiegelberg Stelzer, 2015).

Many times there is a common goal between private companies and municipalities, and the issue then might not be that there are different interests but that the risks of a particular solution might remain hidden. These hidden risks might, if they were known, have created some conflicting interests.

Another side of the smart strategy is political, and how politicians approach and deal with the many smart solutions that are proposed, with perhaps a limited knowledge on the technology involved and getting the information from a sometimes biased source. When asked what the role of the politician is in the smart strategy transformation Jensen describes:

> "It's a very broad category to say politicians. In most planning you have this odd amalgam of some technical, social and natural science…people with different backgrounds. The people that are higher up, they're just as political as the formal politicians. They operate in the same way. They are watching their constituencies, they oversee large groups…and Copenhagen's a big place. I think they're the second largest employer in the country, after the state, with about 44 000 people working for them. And their planning department is huge…and the planning department doesn't talk with the operation dep. very much…the different levels don't talk very much. So, when you talk about politicians you don't necessarily focus on the formally elected like the vice mayor or people in the city council.

> So for the most part, the pure politicians, the ones that are elected, they don't understand the tech at all. No idea. They rely on experts to tell them what's vile. What I think makes them excited is this idea to see the real…this is really what's going on. To have a dashboard and be able to fiddle with stuff. This is the vision that they give to mayors, this is why mayors all around the world get wood for smart cities. So IBM comes in and says: "you'd be able to fine-tune your policies, and see everything and know exactly"(Jensen, 2015).

It's easy to understand why politicians (and others) get excited by ideas like this, and how difficult it can be to object to these types of solutions if the security of the system is assured. He goes on to say:

> "I think the political class both inside the planning institutions themselves and also the formal politicians, are in a very unenviable role. Because they've got one hand: definite possibilities for efficiencies, better services, for opening up the architecture for the city, there's good stuff. But they don't have a full appreciation for the vulnerabilities and weaknesses that come from this, and sort of where things can go wrong. I think that's a problem, because they're making a decision in an asymmetric space, because there's so much on the plus right now and that's what they weigh. You see a scale, but you don't see the thumb on the other side. But it'll come, I'm fairly confident of that…that people will start to see this. I think that we'll head down the trough of disillusionment within about a year or two"(Jensen, 2015).

On the basis of the smart city concept, the role of data in decision making is an important point:

> "There's another piece to this, which people don't pay very much attention to as well, both in research and practice side, is that one of the assumptions that comes through all the smart cities is that with better data we make better decisions. Well, the empirical evidence says exactly the opposite…it's overwhelming. More data typically makes us make poorer decisions, because what happens is our brains become overwhelmed and we typically tend to look at what other people are doing. We don't look at what the data does, because you can't make sense out of it" (Jensen, 2015).

What's being disputed here is not whether data is useful for various solutions such as advanced traffic planning, but whether it's a fundamentally important ingredient of decision-making and to what degree it simplifies the decision making process:

> "When you think of a city, it's a complex organism with so many layers, and there's so much stuff happening inside of that. The simplification that comes out of a lot off the smart city thinking is…the logic sounds like this: "we have a problem and the problem is e.g. traffic congestion, air pollution, climate change, resource consumption, something like that

> or some combination thereof. And we don't have enough data to understand what to do. Ok? That's the first starting place. The next step is; what sort of data do we need? We need all kinds of data, on parking and mobility and etc. Then once we have that data that we want, we're able to make policy on the basis of that data." Therein where everything dies. Because policies are not made on the basis of data. Data is one piece off a complex equation, like this long algorithm… maybe 40 or 50 characters long, and there's all these kinds of operations inside of that. A complex piece, and the data comprises one of those. That's it, it's just one. It's not even the most important one…vision, belief, what do you think…those count much more than data"(Jensen, 2015).

The complexity of a city further enhances the difficulty of a sustainability transformation, and Copenhagen is an example of a city where the structure sometimes make change slow and asymmetrical:

> "If we look inside the municipality, we're used to work in silos and it's difficult to work across the silos…because people are fixed on their projects and on their goal and it's not so easy to create cooperation between the silos. Sometimes you have two different solutions but it would have been better if they were combined from the beginning. Also in Copenhagen we have 7 administrations with 7 mayors from different political parties so it's not always that easy. But we're trying and smart city solutions, that's one of the ways to do it and get closer in this cooperation. And then like we talked about with private companies, sometimes we have different set-ups that makes it hard to cooperate, but everybody is willing to do it and we are putting a lot of effort into it…because we can all see that it's the right way to go"(Spiegelberg Stelzer, 2015).

5.3.2. Wi-Fi & Bluetooth Tracking

Moving on to the actual tracking system, Mayor Kabell describes his view on how the data collecting is making Copenhagen a smarter and better city:

> "I think it is a great possibility we have now to use data to make the city greener and smarter. But I think it is important to differ between what kind of data that are collected. I have no problem with collecting data that are not tied to an individual person. When we use traffic cameras to count the amount of cars and bikes etc., and the data is processed in the cameras, I think it is a good use of the technology. But if we need to store data over time to map the individuals travel through the city, it is important to secure the data in a way so it cannot be traced back to the individual person. If this is not possible (I'm am not a technician), it is important that people accept that data are collected, before we collect them" (Kabell, 2015).

Based on this it can be said that Kabell believe that it's important to make the data collected untraceable back to the person, but also that consent is only is necessary if the data collected isn't anonymized. Moving on, the traffic department explain the purpose of it and what it is aimed at as follows:

> "In Copenhagen we have a high priority on optimizing our signal plan and reducing the travel time on some pre-specified corridors. As goes for H.C. Anders Blvd., we needed to measure our travel time in the H.C.Anders Blvd. in order to be able to model this corridor to optimize our signal plan. Moreover, after setting up of the new signal plan we needed to have data to evaluate our models and see whether we were able to reach our service goal for reducing travel time for cars. One of the main aspects of BT/Wi-Fi tracking is that the sensors are very cost effective in compare to other existing travel time measurement technologies. Each sensors can cover both traffic direction and a wide road with more than 4-6 lines on each side, moreover, these sensors are non-intrusive meaning that they will be installed on the roadside and there is no need to change the road infrastructure to install them. Correspondingly, there is no need for maintenance similar to loops (e.g. changing the wires) or cameras (e.g. cleaning the lens). There are also a large number of users who carry various devices (phone, radio, navigator etc.) that have either BT or Wi-Fi communication capability. This enables us to gather data without requiring to invest on buying some on board units (OBU) or RFID tags etc." (Van Vlerken, 2015).

As said before a Wi-Fi and Bluetooth system offer very effective and low-cost data collecting, and can be very helpful in advanced traffic planning, not only because of how easy it is to implement. The mayor of the Technical and Environmental administration, Morten Kabell, also sees great potential in this project: "There is a huge amount of possibilities in using the data – from planning the individual travel to managing the traffic" (Kabell, 2015). The data collected can according to the concept of Copenhagen Connecting be used for other purposes:

> "Ability to sell aggregated, anonymous data to private companies based on accurate flow data throughout the city. Location-related data and more detailed raw data can be sold to private stores and restaurants for use in their marketing ex. where are their customers originating from and where do they live in the city. Location based services can offer push messages to citizens about just-in-time special offers in the area. Finished analysed data that is combined with other relevant data sources could be valuable for the assessment of where to open a new restaurant or store and its likely profitableness based on historical data about the behaviour in that area and knowledge from the opening of other similar restaurants" (Copenhagen Connecting, 2013c).

When the subsequent data use is more unsure, as it is in this example, the security of the citizens seem to decrease, since they have less control of what the data is being used for. Added to this is the fact that citizen consent isn't a part of the system further increases this issue. Stephan J. Engberg, who is an internet researcher active within the EU, analyses the situation:

> "as to what they're doing, they distribute a daily key to all their sensors, which they use to mingle in some kind of algorithm with the MAC-addresses, in such a way that they create the same, the right key for every device, but they change on a daily basis. And there is some reason why they do this, because so two different sensors will have to be able to create the same derived key from the same mac addresses. Because otherwise they can't track you. So what is this? They have the keys, so they can always go back and track you if they wanted to, they can go back and issue fines five years back and take your driver's license because you're speeding again. They have the knowledge to do that. They can claim that they're deleted but that's not credible. That's point one. Point two, it is an internal security thing. And what they do internally does not change the problem of collection in the first place. It's what we will call "privacy friendly best case" (Engberg, 2015).

The legally of the tracking system has been disputed, ending with the DBA ruling that said that it was not breaking EU regulation. This ruling is according to Engberg incorrect, and to a question wondering what part of the system that is illegal he answered:

> "It is the collection itself. And you have to see the background. First of all, the main problem is that the Wi-Fi is designed wrong, it's designed so that it reuses the same identifier – that's digital pollution, okay? Because it correlates, it links transactions that shouldn't be linkable. That makes you trackable by design. Even though you don't have to. Tracking you or making you trackable is the problem in itself. So, the mobile phones are not designed to be secure or to help you, they're designed to track you. Okay? Now you have to see the regulation in context, because the EU data protection regulation originally was revised around 2002, and it has built in mechanism such as proportionality and things that could sort of say "okay we are not really precise here, so we hope that the data protection agencies and authorities can actually manage this." Very fast we realized that it didn't work. So in 2009 they did what they called the E-privacy directive. The E-privacy directive is a refinement and an improved precision in some core elements of security. That is that you are not allowed to recognize a citizen unless they have consented prior to the recognition. Okay? You are not allowed to identify people and then resolve whether you're allowed to identify them. It's not ok" (Engberg, 2015).

The DBA emphasized in their ruling that the system is anonymizing, hashing, the MAC-addresses and by doing that is law abiding, but judging by this statement by Engberg you can get the impression that these procedures don't matter since the it is the collection itself that is illegal but he continues and addresses whether anonymisation and hashing matter:

> "Of course it does, but not according to that regulation (the E-privacy directive). According to the data protection regulation, the general data protection regulation, it matters what they do to the data. But according to the E-privacy directive they are not allowed to collect it in the first place. Okay, so, it's two different parts of regulation that we are talking about. And you have to understand one thing, the data protection regulation is designed very carefully in the sense that you are not able to provide a general consent to use your information for things you don't know about. And what does that mean? It's liberal in the sense that you are allowed to do whatever you want; (...) you can run around screaming your social security number and doing whatever you want, as long as you're only hurting yourself. That's the liberal part of it. But the regulation is created in such a way that the receiver of information is bounded by the purpose and informed consent. And it means that they are required to assure that the data they collect, the personal data they collect, is specifically limited by an informed consent or a specific purpose. And as soon as that purpose is done, they have to anonymize the data. That's the general data protection regulation. Now the E-privacy directive doesn't even allow you to do that, because things like anonymisation and pseudonymization is a lot harder regulated in the E-privacy directive. You don't have proportionality, you don't have authorities' rights to say "well, this is okay because it's for the better good." No, it's not part of it. Because that's where the data protection regulation failed. And what they are doing here is that they are trying to claim some kind of pseudonymization, after the collection. And that concept is dead. It's an excuse for abuse is what we call it, and we can't design a world like that" (Engberg, 2015).

When Engberg describe the legal issues with the Bliptrack Wi-Fi and Bluetooth tracking system, it seems very clear that its legality is uncertain. It can then be asked how the DBA decided to allow it, given these legal issues:

> "It's because it's run by bureaucrats. And there are two problems here; one is that they don't know enough about what they are doing, and the second is that they have interests. They think these interest are more important than the problems they create. For instance, they claim that it's ok that they track people in traffic because that can make them do some kind of advanced traffic management, or whatever. And they claim that the damage to the citizen is less than the benefit to society. That is sort of the general excuse that bureaucrats always have used. But it's wrong. That's easy to claim, but it has to be seen in light of the fact that

> they could be solving this problem without that damage. Blip Systems could have used a mechanism that couldn't identify the car. Okay? So, we have technology that just see that here is the car, but we don't know which car it is. That would of course mean that they would have the hardest time detecting…recognizing this car 500 meters down. Because they shouldn't be able to. But that is usually the purpose itself. With most of the congestion they would be able to measure without problem, like speed, instantly, without having to recognize the car itself. And in case that they wanted to know more about how traffic ran through the city, then they have to have more advanced solutions where they actually would have…let's say they make an app to run on the mobile phone so that the consumer would accept that this app is reporting from junction point A to junction point B and the time it took for someone to go this distance, but anonymizing in the way it is being reported. So the need could be resolved without the damage" (Engberg, 2015).

Although the illegality of the Wi-Fi and Bluetooth tracking cannot be completely confirmed by this study, there seem to be substantial uncertainty in its legal foundations. One of the reasons for this is the complicated process of interpreting regulations, especially when dealing with fast-advancing technology. Engberg mentions that there are more advanced solutions that could have been used, that would be legally sound, that result in the same data and could be used for advanced traffic planning. These solutions, though, can be assumed to be more expensive, which means that the citizen get somewhat bargained with between the municipality trying to create cost-effective solutions over those that are fully privacy-assuring and secure.

The traffic department themselves assure that "The city follows all laws and regulations that apply to the subject" (Van Vlerken, 2015).

The MAC-address of a mobile phone that is being transmitted, although unique, can be changed[12] either via an application that runs on the device or via the integrated protocol:

> "If you know a little bit about protocols, you will know that Apple iPhones recently, about a year ago, changed so that it started using non persistent MAC address or what they call random MAC-addresses. So, if all mobile phones, all Wi-Fi mobile devices changed MAC-addresses all the time, you wouldn't be able to correlate two readings of the same device. . So, the mobile phone would never respond to the same MAC-address twice. Okay, so if that was the principle in Wi-Fi, you could do whatever you want. Then the Blip system wouldn't be violating the E-privacy Directive" (Engberg, 2015).

[12] Blip Systems claim in their "Bliptrack Privacy Concerns" page that MAC-addresses can't be modified (Blip Systems, 2015b)

If everybody would have devices that create random MAC-addresses the system wouldn't be able to follow the same device with several sensors, since they would see it as different devices. This would mean that the data collected is legal but would also make the data less usable, because the impossibility of following a person for a long distance. Another presumed problem is what can be called "double-tracking", that a device is seen as two devices and persons by the sensors. This could also further complicate data usage.

Another issue is that of storing hashed MAC-addresses on a cloud server:

> "First of all, no cloud is ever secure. The benefit of cloud is that you can move services from one system to the other. It means that data has to be accessible by the system, and it means that it's not secure, because you can always get below the system and circumvent all security. So, if you put data into the cloud, it has to be secure by design. It has to be un-abusable by design. Otherwise it's not secure, end of story. So, never personal data in the cloud" (Engberg, 2015).

The previous studies on un-hashing MAC-addresses show that, although it cannot certainly be said whether the hashed MAC-addresses that are stored on Blip Systems' servers can be un-hashed, there's a risk that they can. Applying something like the precautionary principle to this, would mean that this risk is too big and that this data shouldn't be stored on cloud servers. Engberg continues:

> "I've been working since 1999 with identity management focusing on how to resolve the apparent contradictions…and there are none. There are no trade-offs between security and freedom, or privacy or whatever we're going to call it. That is not a consequence of bad technology design, or in-optimal technology design. As long as we avoid identifying citizens, which is the core problem, then we can make the balances work fine. And the system works much finer if you don't have personal data at all. They don't need personal data, they need data and that's not the same thing. And what is important to understand is that this is not like we have to give up something to gain security or whatever. It's about questioning how to do it. The solution should be device-side, you should be able to control in the device exactly what kind of information you are providing and it should be so that you are not you are not providing linkable information. That would eliminate abuse-potential. And thereby create what we call digital sustainability to create physical sustainability. And that would be no problem, we can solve this, if we want to. The problem is that they don't want to solve it because they want that kind of control and they already invested some money into it and now they are unable to go back. Because that would mean that they made a mistake" (Engberg, 2015).

What Engberg is calling for is for citizens to have better control on what data they share, which is a reasonable request, given that the collecting is carried out by their own municipality. The aspect of citizen involvement is more extensively analysed in an upcoming segment. Once again, the purpose of the system is crucial when designing it:

> "I think this is a question that does not get asked very frequently: what's the point of this? Typically what you hear coming from the European commission and what you hear from a lot of the political side is: "this is the only way we can handle our resource, limitation and sustainability problems…or this is the best way or the most cost-effective. As if we've exhausted every other policy option in the world, and this is our only salvation. That's usually the justification. Which makes me a little bit nervous because is it for the good of the city or is it for the good of some companies who can sell some gear that would otherwise be worthless on an open market because private companies don't want to pay for their things. Which is it? Or maybe it's some combination of both? And I think asking that question is a good question. But…a city being a city…there's not going to be *an* answer. There will be a multitude of answers that will shift over time, day to day, month to month and year to year" (Jensen, 2015).

5.3.3. Privacy Awareness within the Municipality

As previously declared by Holm Carlsen's study (2014), the privacy aspects are not very prominent in the plans and material describing the concept of Copenhagen Connecting and this remains true, but the question is whether an awareness within the municipality has developed since then. Privacy can be a disruptive, but crucial, aspect when forming a smart city strategy, and this is demonstrated by an experience William Jensen had during the last year:

> "I had a funny moment last year when I was working on the Horizon 2020 application. I was in the room with representatives from different cities and some of the industrial partners, and I just raised my hand and said: "It might not be a bad idea to at least address the issues inside of this, because there are security and privacy issues", and one of the guys who was responsible for shepherding the application through the system came over to me and he's like "we don't want to talk about that right now, because we've had those conversations already and they're really complicated, so don't raise that again." But I don't work for the city, and I don't work for him, so I just nodded my head and said okay." (Jensen, 2015).

This is one example of how a municipality can choose to avoid aspects that "distract" from their focal goals and aspects, which seem to have led to that a bigger discussion of privacy developed. The senior Smart city advisor shares his view of the situation:

> "This idea of tracking people with Wi-Fi, or using this system, I don't think we're actually going to use it in the overall smart city strategy. I mean, not like we install some things so you can where people are moving…we're not implementing that at the moment because it's a huge issue of privacy and big brother society etc., so it's not really at the moment one of the things we are focusing on" (Spiegelberg Stelzer, 2015).

This is of course quite a contrast, since the tracking project in fact is in place, but can be seen as sign of that the structural silos still complicate effective communication and planning. When asked how they came to that decision he adds:

> "It's mainly because we couldn't implement the Copenhagen Connecting concept as a whole, and if you don't implement it all it doesn't make that much sense. It's also because we're in a political system and an administrative system, and we should provide concrete solutions…and it's not that concrete compared to a lot of the other projects that we can work with… Let's say working with the sewage system, the flooding and those problems of Copenhagen. So, I think that's the main reason, it's a bit difficult to go down that road, and we have a big discussion about privacy...that is coming from everywhere…I mean both from ourselves, working in the municipality, from the politicians, and there's a lot of debate in the newspapers and public in general. So, each time we talk about smart city solutions, the first thing people ask is "what about privacy and big brother?" That's why we take it very serious and we have decided to make a privacy board with experts, people who know about technology, communication, IT and ethics…basically. They're experts within the field, and they should guide us to find the right solutions so that we don't go down the wrong path, and create a society where you can watch everybody. We are setting it up at the moment, we have found the people that are going to be in the board (…) and they will have their first meeting in around a month. So it's decided and it's going to be established. And I think it's important that it's people from the outside of the municipality, it has to be someone independent to guide us and give us advice" (Spiegelberg Stelzer, 2015).

The establishment of a privacy board definitively shows that there has been a privacy discussion within the municipality and that they are taking it serious, although it's too early to discuss the actual effects of this privacy board in this study. He goes on to say:

> "When you talk about smart city and intelligent city, it's very complicated and complex, and it's sometimes very hard to explain actually. Like we talked about before…people started think "what about surveillance and big brother" and all this kind of stuff. I think the way to go there is to demonstrate what works. So if you can go out on the street and here we have an intelligent lamp post that can do certain things, then you can really see that this works…better feeling of safety and better traffic security, and then you say "okay that's a

> good idea, let's have more of that, we'll invest in that". So I think the way to go is to demonstrate these things and show them. Start small and then you can scale up after, instead of thinking in big systems" (Spiegelberg Stelzer, 2015).

This offers an inside to why the politicians in the end said no the grand project of Copenhagen Connecting, and how the new strategy of implementing smart solutions now is designed. Mayor Kabell reaffirms that privacy indeed is an issue:

> "The biggest challenge is the privacy challenge. We should not create a surveillance society just to make the traffic go smoother. And we have the obligation to take the discussions now, before we decide what kind of design we will use in the city" (Kabell, 2015).

The Mayor confirms that there's awareness also within the political structure, as the previous statements from the smart city advisor has presented. This means that for the politicians to go through with a project, they have to be assured that the solution isn't threatening privacy or citizen choice, but the question then becomes; assured by who? A private actor that want to sell their products to the municipality, or a municipality worker that might be lacking the knowledge for this particular technology?

Jensen adds to his experience of addressing these issues:

> "I do think at least in Copenhagen specifically, that some of the questions that I've raised around security issues, network security, data security, transparency, openness, ownership, who owns this data and what's it going to be used for… is a bit like farting at a fancy dinner party. Might be funny for one or two people but you're going to piss off (the rest)" (Jensen, 2015).

5.3.4. Citizen Involvement

One of the key factors when working with a smart city and a tracking system is how the citizens are involved and notified. Not only just for legal reasons, where the consent prior to collection is crucial, but also for moral and transparency reasons. The senior Smart city advisor addresses a question on citizen participation in the following way:

> "You can answer that question in many ways because if we would go out right now and ask anyone who lives in Copenhagen about the Copenhagen smart city they wouldn't know because we haven't really involved the public yet, so far. But when we start to implement the solutions, then we'll have a lot of citizen involvement. Where we get them, for example, to use solutions like save energy and be aware of how much energy they are using, and also setting up some apps, for example, where you can choose the optimal bicycle route, and you can see where there's pollution and noise etc. Or you can for example have an app installed so that when you pass a park that is newly rebuilt, then you can evaluate it and give your

> comments. Or before we built it you can say what you would like to have in that place. And we will also have an engagement portal where you can come up with ideas for smart city solutions. But at the moment, so far, we haven't really focused so much on the involvement of the citizens. Of course the users of all our solutions and the solutions we create but not in the development of it so far. I have to admit it" (Spiegelberg Stelzer, 2015).

Van Vlerken, academic assistant at the Technical and Environmental Administration, adds that "Citizens are informed through press materials" (Van Vlerken, 2015). This press materials can however be quite lacking as they avoid to specific information, e.g. exactly what data they're collecting, the location of the system, how to opt-in/out et cetera. This 'minimalistic' approach to citizen involvement, does not have any major support of the smart city theories that have been presented in this thesis, since they more than often weigh citizen participation heavily compared to other city characteristics.

To mayor Kabell there's an essential connection between the smart city and its citizens:

> "The smart city is made for people. We do it to make things go smoother for the individuals, and to give more possibilities. Therefore the individual has the essential role in the transformation" (Kabell, 2015).

This confirms the role of the citizens in Copenhagen Smart city as more or less passive, with the municipality on the other hand collecting data to create smart solutions. Engberg problematizes the meaning of smart in citizen choice:

> "does smart means that some system is smart and tries to make choices on your behalf without understanding it, which is 99 % of the cases, or does smart mean to have structures so that we can actually talk to each other and get these mechanisms to work but distributing choice and control to the citizen, and having the intelligence to distribute it to your hands on your questions. That's a huge distinction! And if you look to the smart programs around right now, including the one in Copenhagen, none of these have sustainability in mind. They all focus on one aspect that they think they want, and the solution to that is always the same –collect some citizen information and then try to make some intelligent solutions" (Engberg, 2015).

Jensen proceeds on the topic of citizen involvement and transparency:

> "This is, I think, the biggest problem, that they're not telling people and they're consciously not telling people. That is by design…that is not an accident. That is by design because they don't want these questions, because they don't want people to know. And that's here, that's in Copenhagen. This is in one of the most democratic, transparent and the least corrupt countries, right? So, you have a city architecture that says: "no no don't tell anybody, just

> take it". Because if they inform people, then people won't want to do it. And what does that tell you about what you're trying to do?" (Jensen, 2015).

The choice for citizens that don't want to share their data right now is to opt out of the system:

> "They can choose not to participate by turning off Bluetooth "Discoverable Mode" and Wi-Fi on their mobile devices while travelling through the site" (Van Vlerken, 2015).

This is unfortunately problematic since the area where the collecting is happening isn't known to the citizens, and there aren't any signs that indicate that a collection is going on. If there was a sign, it can be claimed that people can opt out by choosing a different route that isn't in the affected area, but given the fact that this is in the very central parts of Copenhagen and that the affected roads are some of the most trafficked, the sensors can be hard to avoid without severely affecting convenience. This is especially true after the expansion of the project area.

Another point is that; even if there was a sign that informed that the data collection is happening and that the data is being used to create a better city, it's hard for the citizens to make a choice, because they don't know the consequences and how the data might be used further on. So, increasing the data control for the citizen might be more "smart" than keeping the controlling power within the municipality:

> "So, instead of centralizing all this data in structures that are both inefficient and insecure, you distribute it. And you put the control in the hands of those that would become vulnerable. And you get access to much more data, because I know much more about me than you will ever do in some central system. And the systems will adapt to your needs, instead of adapting you to the systems, how you need to make very flexible structures or how to manage society. So, fundamentally you can say that, I am very much anti command and control. Which is about what I as an intelligent city do to you as a stupid citizen. The fact is the exact reversal, it is the citizen that is intelligent on their own needs and in their mind, and the rest of the system needs to adapt to your needs because we cannot know what your needs are" (Engberg, 2015).

Putting data control in the hands of citizens would mean that those who want to share their data can do so, without compromising with those who doesn't want to. But to realize that this is a problem that needs to be addressed can be a difficult step.

5.3.5. Analysis based on the Theories of Surveillance

Now that the research questions have been gone through one by one, we can return to the theory and analyse the results based on the operationalization presented in chapter 4. This analysis is presented in table 2.

Table 2. Displays the surveillance characteristic that is being analysed and a description of how it applies to the case of Copenhagen.

Surveillance Characteristic	Description
Known to the individual	The Wi-Fi tracking system of Copenhagen is not widely known among citizens and therefore people are not adjusting their behaviour as a response to it. This is then again not the purpose of the tracking system, at least not at this stage.
Unknown in specific time	This characteristic assumes that the surveillance is known, and as this is not the case in Copenhagen, it loses its purpose. For the ones that do know of the project, there's no way of knowing when data is being collected other than that it's happening constantly. In this sense, the watcher is not visible.
Uncontrollable by the individual	The system in Copenhagen allows the individual to opt out by turning off the Wi-Fi and Bluetooth discovery mode, which does offer a way for the individual to control the data collected, but since the system isn't communicated very strongly, this opt out option remains hidden to citizens.
Mechanized and Automated	A Wi-Fi based tracking system works and stores data without any necessary human supervision, which is one of the main benefits of the system, compared to e.g. traditional ways of counting cars.
Geographically Centralized or De-centralized	With modern data transfer and cloud computing, it's easy to analyse data anywhere, that's been collected anywhere. So, the geographical structures of Bentham's panopticon are outdated, as the system in Copenhagen is based on cloud computing, making analysis of data possible in a much less restricted geographical area.
An aim (ambition) of being transparent	The ambition of being transparent is evident in the case of Copenhagen, for example through the creation of an open data platform, but the specific Wi-Fi and Bluetooth tracking project doesn't display any mayor transparency. Some improvements would be to present to citizens specifically what data they are collecting, in what area and how to opt out.
Scalable	Low cost and easy installation are two of the factors that make Wi-Fi tracking systems easy to scale up, which not only wouldn't affect any of its characteristics but on the contrary increase the ability and functions of the system.
Collectivistic and non-hierarchical	The hierarchical structure of the tracking system is clear; the municipality is collecting data on citizens to help the city come up with smart or sustainable solutions. Because of the inability of citizens to view their own data that's been collected, or any data for that matter, this characteristic doesn't resonate much in Copenhagen. This is of course also affected by transparency. The reason for having a collectivistic tracking system is on the other hand hard to see.
Non-specific in its data-gathering	The tracking system is specific in that it only cares about location over time, though this might be more for technical reasons than an active choice to only collect specific data. It's non-specific in that it's still unsure exactly what the data will be used for, and how.

Directed towards controlling and adjusting the disobedient	The purpose and function of the tracking system is to get an improved image of people's movements in the city, and using this information to come up with solutions and plan traffic flow. So in this way, it does have a specific purpose, unlike panspectrism and more like panopticism and informational panopticon. The difference is that they are not trying to change behaviour directly by telling people about this system and have them adjust, but instead changing behaviour via solutions based on this new information they've collected. Another difference is that Bentham and Foucault's concepts had disobedience management in mind while the tracking system has urban issues and inefficiencies in mind – though if you see environmental harm and urban inefficiencies as a form of disobedience, and the work directed towards managing and reducing these as one unit, the differences start to vanish. This can be called the e*nvironmental panopticon* – data collection and surveillance for the good of the environment and/or the city. The concept of Copenhagen Connecting can more successfully be compared to panspectrism, seeing its wide data collection without the specificity of the tracking project.

6. Discussion & Conclusions

This chapter will include a discussion of the results of the case study, as well as the concluding remarks.

This study has been an effort of getting a comprehensive view of the Wi-Fi and Bluetooth tracking project in Copenhagen, as a part of their Smart city strategy. In order to get this width, a wide variety of sources has been used from both inside and outside the municipality. In hindsight, more focus on the ITS program might had been appropriate, as the specific tracking project is a part of this program, but at the same time it's also described as a part of the concept of Copenhagen Connecting.

One essential point to understand is that the issues and aspects that have been covered by this study not are isolated from each other, but conversely are dependent of and affect each other. Privacy seems to be becoming more and more unavoidable for Copenhagen to deal with, and the awareness of it in the municipality seem to have changed over the last year, much because of the debate that's surfaced. To deal with the privacy issues that might exist, one must also deal with the transparency, as well as the citizen participation. We can't create a transparent city without involving citizens, if only just by effective and sufficient communication, and we can create a privacy aware city without being transparent with our solutions.

It's important to understand that this study is not about trying to label something as surveillance or not, or trying to find when something becomes surveillance, as this quest many times lead nowhere and is counterproductive. It can also be noted that surveillance is relative and personal, depending on the individual affected. Instead the study aims to analyse how the smart city operationalizes sustainability in a particular case, and how it positions itself relative to transparency, citizen choice and participation, and privacy.

As hard as it is, the difficulty of defining and concretize privacy shouldn't stop us from studying and analysing it, especially when modern technology allow for unprecedented data collection on our lives. This point is further strengthened when cities initiate this type of collection, and create partnerships with companies that function on the basis of collecting and selling behaviour data on private people. The step of the municipality to partner with a private company in this type of activity, which includes private information, is fundamental, and need to be further studied. The role and service of the municipality is changing, and how this will affect citizens in the long term is of course hard to speculate.

What's easier to say is that the citizen has a crucial role in any major urban transformation, and especially those that are based on the collection of citizen data. As stated in the introduction

of this study, according to a survey in the US, 82 % of the asked thought that the disclosure of their physical location over time was either very sensitive or somewhat sensitive, which tells us that if we want to pursuit a city structure based on data collection, we must tread carefully and in a balanced fashion. One of the reasons for this is that many of the technologic solutions that make the smart city are hard for the average citizen to understand, and this is also the case with Wi-Fi and Bluetooth tracking. It's hard for the citizen to understand the possible risks or consequences (often because it's unclear what the data will be used for), and to create a personal opinion on such a project when they're in an environment that's lacking in knowledge or is biased. This is why putting up a sign that explains that the city is collecting data on your location for the good of the city or environment isn't a complete solution to the problem. To fully address the problem, a systematic strategy of addressing transparency, citizen choice and participation, openness and other aspects that have been addressed in this study, has to be created. All of these are cornerstones for digital sustainability, which will enable physical sustainability.

With the revelations of Edward Snowden, that the NSA and various other countries –one of them being Denmark, are involved in several global surveillance programs, and the increased data collection from Google, Facebook and other social interaction platforms, it is extra important for cites to stand firm on the principles of the privacy and integrity of their citizens, and not compromise the very heart of a city – its citizens.

The smart city is facing a crucial intersection that will determine whether it can be a strategy that accomplishes the integration of physical and digital sustainability in society, or fails to do both, and this has to do with how it approaches change and solutions. If the *smart* premise is that all that's missing in successful city planning and strategy is data and technology, one can argue over how smart it really is. If the premise is that success depends on involving citizens in the transformation, and leaving choice up to them, it's harder to fault or criticise solutions, because it's coming from bellow as well as from above. One road relies on the intelligence and knowledge of the municipality and hopefully benign private companies because they claim to know what solutions is demanded - based on collected data, and the other relies on that a sustainability transformation never means that the citizen is stripped of the choice to participate.

6.1. Conclusions

Although the smart city concept can seem very new and fresh, the idea is far from it[13], in the light of the fact that the concept revolves around what role technology has in an urban area. The

[13] Some of the concepts with similar traits are: the intelligent city, digital city, wired city and the networked city.

smart city has previously in the study been compared to a smorgasbord or a buffet of features that can be included in the city strategy, where some cities choose to focus a lot on resilience, others more on citizen participation, and so on. Copenhagen has been shown to focus more on climate change, with their goal of being CO_2-neutral to 2025, private business partnerships, and the digital infrastructure in the form of the vision of Copenhagen Connecting. They have on the other hand chosen to focus less on citizen participation and choice in this transformation, in contrary to much of the smart city theory. This further enhances the smart city concept as a buffet of features that are not all obligatory.

It can also be concluded that although Copenhagen uses the Smart city concept as to tool to reach their 'real' goals, such as becoming CO_2 neutral to 2025, the use of Copenhagen Connecting as a vision for the city, consolidates the Smart city and all of the solutions that come from it, into Copenhagen. This means that the effort of creating a distance between Smart city Copenhagen and the 'real' Copenhagen is reduced.

The interviews have showed that there's a wide variety of opinions on the development that Copenhagen has initiated, with their smart city strategy and the Wi-Fi and Bluetooth tracking project. The reason for this is how a number of issues and aspects are approached from the municipality, and the standpoints in relation to these. One of these is privacy, where there seems to have been a change in the debate in and around the municipality of Copenhagen. It has not yet changed the communication of the smart city to its citizens, in publications and such, evident of an acquiescence of privacy integration in the city strategy. This has sparked the creation of a privacy board, which it's too early to give a verdict on, but at least shows that privacy is moving up the ladder of priorities in Copenhagen, if only in a structural way. The aim should of course be to make it a priority also in praxis, and have it included in future projects on several levels.

The Wi-Fi and Bluetooth tracking system itself, stand on unclear legal ground, because of the collection of MAC addresses without the consent of citizens, although it was for now deemed legal by the Danish Business Authority. The ruling weigh the hashing of the MAC addresses as being enough to completely anonymise the citizens, but whether this in fact is true also remains unclear.

When it comes to transparency and openness, they are also lower down the list of priorities as regards to the Wi-Fi and Bluetooth tracking project, as the function and more specific information isn't adequately communicated to the citizens. This is also affected by the design of the system, based on that a Wi-Fi and Bluetooth tracking system which collects MAC

addresses have unclear legal issues, possible private data security issues, and at times can take choice away from citizens (the choice to participate or not). If Copenhagen is serious about creating a Smart city, they ought to move away from the centralistic smart approach (the city collect data, and come up with solutions together with private companies) to a collectivistic (the city collect data that the citizens has given their consent on giving i.e. opt in, and come up with solutions with all actors involved, including citizens).

6.1.1. Further Studies

This study has contributed to the topic by giving some inside into the process of creating a Wi-Fi and Bluetooth tracking system within a smart city strategy, and some of the issues that can surface when establishing such a system. What it doesn't cover is the opinion of the citizens of Copenhagen in relation to the tracking project, and what *their* feelings are about it. The relation between private actors and public open data platforms is also in need of more studies, as well as studies investigating the legal perspective of new data collection methods. Generally, more studies are necessary in the area, as more and more cities turn to these type of solutions, with several of these being in Denmark and Sweden. To fully understand a sustainability process it's always necessary to question why a project is happening, and how it fits into the long term strategies of the city. For this reason, a continuum of studies within this subject is crucial, and will improve the learning curve so that cities that want to invest in technologic solutions in the future don't make the same mistakes. This would be another step down the path towards sustainable city development.

Acknowledgements

I would like to thank my supervisor Stefan Larsson, with whom I've shared valuable discussions that has given an increased depth to my thesis, as well as steered me in the right direction. I would like to thank all the informants that have participated in the study; William Jensen, Kim Spiegelberg Stelzer, Stephan J. Engberg, Søren Kvist, Morten Kabell, Magnus Boye, Jos Bo van Vlerken, Thomas Højlt and Emil Tin. I would also like to thank Johanna Alkan Olsson, who convinced me to choose tracking in the sustainable city as the topic for my thesis. Thanks to Alex and Tanja for the comments. Finally, I would like to thank my classmates Hanna Matschke Ekholm and Josefin Methi Sundell, for the many discussions we've had during the writing process.

References

Personal interviews

Boye, M. (2015). Internet interview. 2015-05-12.

Jensen, W. (2015). Personal interview. 2015-04-22.

Engberg, J. S. (2015). Internet interview. 2015-04-16. Via Skype. Recorded with Talk-Helper.

Kabell, M. (2015). Email interview. 2015-05-12.

Kvist, S. (2015). Telephone interview. 2015-04-14.

Spiegelberg Stelzer, K. (2015). Personal interview. 2015-04-23.

van Vlerken, J. B. (2015). Email interview. 2015-05-08.

Other Sources

Abedi, N., Bhaskar, A., & Chung, E. (2013). Bluetooth and Wi-Fi MAC address based crowd data collection and monitoring: benefits, challenges and enhancement. In 36th Australasian Transport Research Forum (ATRF), 2-4 October 2013, Queensland University of Technology, Brisbane, QLD.

Bailey, C.A. (2007). *A guide to qualitative field research*. (2. ed.) Thousand Oaks, Calif.: Pine Forge Press.

Becker, H.S. (1998). *Tricks of the trade: how to think about your research while you're doing it*. Chicago, Ill.: Univ. of Chicago Press.

Bennet, A. (2001) Case Study: Methods and Analysis, p.1513-1519, from Smelser, N.J. & Baltes, P.B. (red.) (2004). *International encyclopedia of the social & behavioral sciences [Electronic copy]*. Amsterdam: Elsevier.

Bentham, J. (2002). *Panopticon: en ny princip för inrättningar där personer övervakas*. Nora: Nya Doxa.

Blip Systems (2015a) About. (Retrieved from http://www.blipsystems.com/about/ 2015-05-11).

Blip Systems (2015b) Bliptrack Privacy Concerns. (Retrieved from http://www.blipsystems.com/wp-content/uploads/2014/10/BlipTrack-Privacy-Concerns.pdf 2015-05-11).

Blip Systems (2015c). Bliptrack Wifi Traffic Sensor. (Retrieved from https://web.archive.org/web/20150204144145/http://www.blipsystems.com/bliptrack-wifi-traffic-sensor/ 2015-03-19).

Blip Systems (2015d).The New BlipTrack Indoor Sensor Now Comes in Two Colors. (Retrieved from http://www.blipsystems.com/bliptrack-indoor-sensor-new-color/ 2015-05-11).

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662- 679.

Boye, M. (2015a) Udbredt system til trafikovervågning er ulovligt. Version2 (Retrieved from http://www.version2.dk/artikel/udbredt-trafikovervaagningssystem-er-ulovligt-76565 2015-05-07)

Boye, M. (2015b) Nytolkning af cookie-direktiv er bombe under dansk succesforretning med trafikovervågning. Version2. (Retrieved from http://www.version2.dk/artikel/omstridt-eu-direktiv-er-bombe-under-dansk-millionforretning-76635 2015-05-07)

Boye, M. (2015c). København sætter 'ulovlig' trafikovervågning på pause. Version2. (Retrieved from http://www.version2.dk/artikel/koebenhavn-saetter-ulovlig-trafikovervaagning-paa-pause-76867 2015-05-07).

Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000, September). The vision of a smart city. In 2nd International Life Extension Technology Workshop, Paris.

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

Campbell, S. (1996). Green cities, growing cities, just cities?: Urban planning and the contradictions of sustainable development. *Journal of the American Planning Association*, *62*(3), 296-312.

Copenhagen (2012a). CPH 2025 - A Green, Smart and Carbon Neutral City. The technical and Environmental Administration, draft June 2012. Formula. (Retrieved from http://subsite.kk.dk/sitecore/content/Subsites/CityOfCopenhagen/SubsiteFrontpage/Business/Growth_and_partnerships/~/media/F5A7EC91E7AC4B0891F37331642555C4.ashx 2015-04-20.)

Copenhagen (2012b). Copenhagen: Solutions for Sustainable Cities. October 2012, 2nd edition. (Retrieved from http://subsite.kk.dk/sitecore/content/Subsites/CityOfCopenhagen/SubsiteFrontpage/Business/~/media/9E5C396089DA478D906A77C16C52F3AF.ashx 2015-04-25).

Copenhagen (2013a) Vedtaget Budget 2014. KØBENHAVNS KOMMUNE.

Copenhagen (2013b) Copenhagen Smart City. Københavns Kommune. (Retrieved from http://cc.cphsolutionslab.dk/_include/img/work/full/SmartCities_2013_A4.pdf 2015-04-09).

Copenhagen (2014) 8 New Intelligent Traffic Solutions. City of Copenhagen. The Technical and Environmental Administration. (Retrived from http://kk.sites.itera.dk/apps/kk_pub2/pdf/1205_zA7aIS8D1d.pdf 2015-05-12)

Copenhagen (2015). Om - Åbne Data fra København Kommune. (Retrieved from http://data.kk.dk/about 2015-04-10).

Copenhagen Connecting (2013a) Copenhagen Connecting – A unique and innovative opportunity to shape the future of Copenhagen. PowerPoint-presentation, Sören Kvist. (Retrieved from http://itek.di.dk/SiteCollectionDocuments/CopenhagenConnecting-UK_horizon2.pdf 2015-04-09).

Copenhagen Connecting (2013b) Bilag 9 - Udtalelser fra Eksperter. TM82B7. (Retrieved from: http://cc.cphsolutionslab.dk/_include/img/work/full/TM82B7_-_ekspertudtalelser.pdf 2015-04-10).

Copenhagen Connecting (2013c) TM82B4 - Use Cases - Anvendelsesområder. (Retrieved from http://cc.cphsolutionslab.dk/_include/img/work/full/TM82B4_-_Anvendelsesomraader-use_cases.pdf 2015-04-10).

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

Cunche, M., Kaafar, M. A., & Boreli, R. (2014). Linking wireless devices using information contained in Wi-Fi probe requests. *Pervasive and Mobile Computing*, *11*, 56-69.

Danish Business Authority (2015a) Trafikovervågningssystem ikke omfattet af cookie-reglerne. (Retrieved from https://erhvervsstyrelsen.dk/trafikovervaagningssystem-ikke-omfattet-af-cookie-reglerne 2015-05-07)

Danish Business Authority (2015b) Afgørelse . 26. march 2015. (Retrieved from https://erhvervsstyrelsen.dk/sites/default/files/media/afgoerelse_-_blip_systems.pdf 2015-05-07)

Danish Business Authority (2015c) About- Mission and Vision. (Retrieved from http://danishbusinessauthority.dk/about 2015-05-07).

Demir, L. (2013) Wi-Fi tracking: What About Privacy. Mobile Computing.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

European Commission (2014) 2014 – Copenhagen. (Retrived from http://ec.europa.eu/environment/europeangreencapital/winning-cities/2014-copenhagen/index.html 2015-05-14).

EU-Smart Cities (2014a) PLEEC. . (Retrived from https://eu-smartcities.eu/related_web/pleec 2015-04-09).

EU-Smart Cities (2014b) Transform. . (Retrived from https://eu-smartcities.eu/related_web/transform 2015-04-09).

EU-Smart Cities (2014c). 7570. (Retrived from https://eu-smartcities.eu/commitment/7570 2015-04-09)

EU-Smart Cities (2014d). 5018. (Retrived from https://eu-smartcities.eu/commitment/5018-0 2015-04-09)

EU-Smart Cities (2014e). 7422. (Retrived from https://eu-smartcities.eu/commitment/7422 2015-04-09).

Foucault, M. (1995[1977]). *Discipline and punish: the birth of the prison*. (2nd Vintage Books ed.) New York: Vintage Books.

Foucault, M. (2003). *Övervakning och straff: fängelsets födelse*. (4., översedda uppl.) Lund: Arkiv.

Gerring, J. (2007). *Case study research: principles and practices*. New York: Cambridge University Press.

Giannotti, F., & Pedreschi, D. (2008). *Mobility, data mining and privacy: Geographic knowledge discovery*. Springer Science & Business Media.

Golle, P., & Partridge, K. (2009). On the anonymity of home/work location pairs. In *Pervasive computing* (pp. 390-397). Springer Berlin Heidelberg.

Greenstein, B., Gummadi, R., Pang, J., Chen, M. Y., Kohno, T., Seshan, S., & Wetherall, D. (2007). Can Ferris Bueller Still Have His Day Off? Protecting Privacy in the Wireless Era. In *HotOS*.

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

Holm Carlsen, L. (2014). The Location of Privacy - A Case Study of Copenhagen Connecting's Smart City. Roskilde University. (Master's Thesis).

Hornborg, A. (2001). *The power of the machine: Global inequalities of economy, technology, and environment*. Rowman Altamira.

IBM (2013). Copenhagen Report. IBM's Smarter Cities Challenge.

Kullenberg, C. (2009). The social impact of IT: Surveillance and resistance in present-day conflicts. How can activists and engineers work together, p. 37-40, *FiFF-Kommunikation*, 1/09.

Kullenberg, C. & Palmås, K. (2009) "Contagiontology", in Eurozine. First published in *Glänta* 2008, no. 4.

Lindqvist, J., Aura, T., Danezis, G., Koponen, T., Myllyniemi, A., Mäki, J., & Roe, M. (2009, March). Privacy-preserving 802.11 access-point discovery. In*Proceedings of the second ACM conference on Wireless network security* (pp. 123-130). ACM.

Low, N. (2005). *The green city: sustainable homes, sustainable suburbs*. (1. ed.) Abingdon: Routledge.

Lyon, D. (1994). *The electronic eye: the rise of surveillance society*. Oxford: Polity.

Mann, S., & Ferenbok, J. (2013). New Media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*,*11*(1/2), 18-34.

Martinez-Balleste, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *Communications Magazine*, IEEE, 51(6). http://crises2-deim.urv.cat/docs/publications/journals/794.pdf

Mayer, J. (2014) Questionable Crypto in Retail Analytics. Webpolicy. (revrieved from http://webpolicy.org/2014/03/19/questionable-crypto-in-retail-analytics/#mac_hashing_fn5 2015-05-14).

Nam, T., & Pardo, T. A. (2011, June). Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times (pp. 282-291). ACM.

Orum, A. (2001) Case Study: Logic, p. 1509-1513, from Smelser, N.J. & Baltes, P.B. (red.) (2004). *International encyclopedia of the social & behavioral sciences [Electronic copy]*. Amsterdam: Elsevier.

Orwell, G. (1949). *1984*. New York: Signet Classic.

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

Partridge, H. (2004). Developing a human perspective to the digital divide in the smart city. In Proceedings of the Biennial Conference of Australian Library and information Association.

Pew Research Center (2014) Public Perceptions of Privacy and Security in the Post-Snowden Era. (Retrieved from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ 2015-05-06).

Ramböll (2013) Copenhagen Connecting: Pre-feasibility Analyse. Revision 3. (Retrieved 2015-04-10).

Redclift, M. (2002). *Sustainable development: Exploring the contradictions*. Routledge.

Rios, P. (2008). Creating "the smart city". (Retrieved from http://demo.ctg.albany.edu/publications/journals/dgo_2011_smartcity/dgo_2011_smartcity.pdf 2015-03-10).

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation (pp. 431-446). Springer Berlin Heidelberg.

Schrank, A. (2006a) Essentials for the Case Study Method - the Case study and the Causal Inference, p. 169-175, from Perecman, E. & Curran, S.R. (red.) (2006). *A handbook for social science field research: essays & bibliographic sources on research design and methods*. Thousand Oaks, Calif.: SAGE.

Schrank, A. (2006b) Case Based Research, p. 21-39, from Perecman, E. & Curran, S.R. (red.) (2006). *A handbook for social science field research: essays & bibliographic sources on research design and methods*. Thousand Oaks, Calif.: SAGE.

United Nations (2014) World Urbanization Prospects, the 2014 Revision [highlights]. Department of Economic and Social Affairs. Published by the United Nations.

Vaidhyanathan, S. (2011). *The Googlization of everything: (and why we should worry).* Berkeley: University of California Press.

Vissak, T. (2010). Recommendations for using the case study method in international business research. *The Qualitative Report*, *15*(2), 370-388.

Yin, R.K. (2014). *Case study research: design and methods*. (5. ed.) London: SAGE.

Zuboff, S. (1988). *In the age of the smart machine: the future of work and power*. Oxford: Heinemann Professional.

Appendix 1

Interview Guides:

Questions to the senior Smart city advisor

- Do you wish to be anonymous in the study?
- What does your job consist of? What do you do?
- What is your vision of Copenhagen in 20 years? (a smart/sustainable city?) Targets? Goals?
- What is Copenhagen Connecting? Copenhagen Capacity?
- How do you find solutions for the city?
- How did you get the idea of Wi-Fi-tracking? Where did the initiative come from? (another actor? How did you come in contact with each other?)
- How does the Wi-Fi-tracking work? Where?
- Are there any plans for expanding the project geographically?
- Are you working with (have you thought of) security or privacy aspects? How? Issues? Challenges?
- How does the Wi-Fi-tracking project fit in the vision of Copenhagen? What can it bring? What's your ambition with the project?
- What is your opinion of making citizens involved in the transformation? Is it necessary? Valuable?

Questions to the traffic department

- Do you wish to be anonymous in the study?
- What does your job consist of? What do you do?
- How does the Wi-Fi-tracking work? Where? Who sets up the Wi-Fi?
- What is the idea behind the project?
- How did you get the idea of Wi-Fi-tracking? Where did the initiative come from?
- Are you doing the project with another actor? Tech supplier? How did you come in contact with each other? How do you see your partnership with Blip Systems?
- Was the demonstration in the fall of 2014 your first measure?
- What data is interesting to you?
- What are you planning to use the data for?
- Who collects the data?
- What data do you collect? (CPR-number) And how? (Just location or in bulk?) Can you see what people are doing on their phones or just the location? How do you choose which data is interesting?
- Who has access to what data?
- Are you working with (or have you thought of) security or privacy aspects? How?
- Do you (or another actor) anonymize the data? How did you come to that decision?
- If the system is abused, who would be responsible?
- Are citizens being informed of the data collection? How? Maybe of what the data is used for?
- Can citizens choose not to participate in the project, and not have their data collected?
- Has the legal rights of CC been analysed?

- How are the residents in the area affected? Is their data being collected?

Questions for William Jensen

- Do you wish to be anonymous in the study?
- Have you worked at the Copenhagen Municipality? What position?
- Where do you work now?
- How do you see the sustainability work that has been done in Copenhagen so far? Important factors? Successes?
- What do you think of the smart city efforts?
- Where do you see Copenhagen in 20 years? (smart/sustainable?)
- The big data of Copenhagen?
- Have you heard of the Wi-Fi tracking project? What is your opinion of it?
- What is a threat to privacy?
- How far can we go for the good of the city? How do we choose what is "good"?
- How is Copenhagen's transformation going? Opportunities? Barriers? Challenges? Threats?
- Questions for politicians

Questions for Mayor Morten Kabell

- What role do you see that the individual citizen has in Copenhagen's Smart transformation?
- How do you think about collecting data on citizens in the purpose of making the city more smart or sustainable?
- What opportunities and strengths do you see with this?
- What challenges and threats do you see?

Questions for Magnus Boye:

- What role do you see that the individual citizen has in Copenhagen's Smart transformation?
- How do you think about collecting data on citizens in the purpose of making the city more smart or sustainable? Who should make that choice? Should it be a choice to have your data (as a citizen) collected by the municipality?
- Do you think that the average citizen is aware of the tracking system?
- Do you know if Copenhagen paused their tracking when the Danish Business Authority said that the tracking was illegal? Did any other cities do this?
- What are some of the issues you as a journalist see with this system?

Appendix 2

Pictures from the field observations:


RETAIL
FOR RENT
PLEASE CONTACT
70 22 25 22
DEAS
ERHVERV
Hamleys
PLEASE CONTACT
022 25 22

beerbar

LUNDS UNIVERSITET