Surveillance and privacy in smart cities and living labs

Galič, Maša

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

SURVEILLANCE AND PRIVACY IN SMART CITIES AND LIVING LABS

Conceptualising privacy *for* public space

Maša Galič

Cover image by Manon Heinsman, © Ars Aequi.
Printed by Optima Grafische Communicatie, Rotterdam

SURVEILLANCE AND PRIVACY IN SMART CITIES AND LIVING LABS

Conceptualising privacy *for* public space

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan Tilburg University
op gezag van de rector magnificus, prof. dr. K. Sijtsma, in het openbaar te verdedigen
ten overstaan van een door het college voor promoties aangewezen commissie in de
Aula van de Universiteit op dinsdag 19 november 2019 om 13.30 uur

door

Maša Galič
geboren te Celje, Slovenië.

PROMOTIECOMMISSIE

Promotores:

Prof. dr. Bert-Jaap Koops, Tilburg University
Prof. dr. Eleni Kosta, Tilburg University

Overige commissieleden:

Prof. dr. Kirstie Ball, University of St. Andrews
Prof. dr. Bibi van den Berg, Leiden University
Prof. dr. Serge Gutwirth, Vrije Universiteit Brussel
Prof. Charles Raab, University of Edinburgh
Dr. Linnet Taylor, Tilburg University

TABLE OF CONTENTS

PART II

ACKNOWLEDGEMENTS

Throughout my education I have found wonderful mentors. From my chemistry teacher at the elementary school, my philosophy professor at the Gymnasium, to my professor of legal theory at the Law faculty in Ljubljana. I am greatly indebted to all of them.

At Tilburg University I have been lucky again. Dear prof. Koops, dear Bert-Jaap, I do not think I exaggerate if I say that you are an intellectual of the highest tier. Moreover, you are one of the most wonderful, honest and generous persons I have ever met. You have been the most critical and at the same time the most supportive and encouraging mentor that I could have wished for. Working for you and with you for the past five years (and, hopefully, more in the future) has been a true pleasure and an endless source of inspiration. I could not have written this PhD and developed myself as a scholar (and person) as I did – and continue to do – without you. I have learned and learned again from you. Hartelijk bedankt.

I have been even luckier. Dear prof. Kosta, dear Eleni, having you by my side throughout this PhD has also been invaluable. At the very beginning of this long journey that is the PhD, you gave me a book of poems by Cavafy, pointing out the one called Ithaca. So, following you and Cavafy, I did pray that the road be long, full of adventures, full of knowledge, and that I would find many a summer morning, when with delight and joy, I would enter harbours yet unseen. I think I succeeded, I certainly experienced the delights and joys of research. Dear Eleni – an esteemed legal scholar, a generous colleague, a dear friend – you have supported me in all of my explorations (be it of privacy, surveillance or human geography), making sure that I do not get lost. Σας ευχαριστώ.

Writing a PhD can be a lonely endeavour. Luckily, that was not the case for me. My PhD was connected to Bert-Jaap's VICI project on 'Privacy protection for the 21st century', so that I was but one member of the self-proclaimed 'VICI team'. I want to thank all of the members of the team throughout the years, including Bo, Bryce, Esther, Jaap-Henk and Robin. Having bi-weekly meetings in the form of razor-sharp discussions, organising panels and workshops, and writing many a paper together was the part of my PhD that I enjoyed most.

Two other members of the VICI team – my paranymphs – merit special acknowledgement. Dear Ivan, my patient and supportive office mate and dear friend, sharing an office with you for almost five years was a pleasure. Continuing to be

your friend outside of the office is something that I truly cherish. And dearest Tjerk – coming into my life as a colleague and staying there as a close friend, you have enriched it more than I can say in this public outpouring of appreciation. With every year that goes by, I cherish and respect you more. Even when you found another job, you kept on reading my surveillance chapters and helped me solve the problems that I encountered. I could not have written this PhD without your support either.

Writing a PhD can also be difficult at times. In those difficult moments, it often helps to physically relocate to another meaningful space. In 2017 (with the financial support of an EU Erasmus+ grant), I had the pleasure to spend a month at the Norwegian Research Centre for Computers and Law (NRCCL, University of Oslo) with prof. Lee Bygrave and his team, especially Samson, Kevin and Urku. The warm welcome, a quiet office of my own and several engaging discussions on (data) privacy and public space, have enabled me to begin writing what I perceived as the most difficult part of my dissertation. Dear Lee, thank you again for taking your precious time to engage in discussions with me and for a wonderful stay at your excellent research centre.

I would also like to thank my esteemed PhD committee – prof. dr. Kirstie Ball, prof. dr. Bibi van den Berg, prof. dr. Serge Gutwirth, prof. Charles Raab and dr. Linnet Taylor – whose academic work was the foundation and inspiration for my own research. I am very grateful that you have accepted the invitation to be in my committee and I appreciate your thorough reading of my dissertation that has provided me with a number of highly relevant and valuable comments.

I would also like to thank Raphaël for helping me find my own 'academic chutzpah'. And for all of those patient discussions during the final year of my PhD that enabled me to greatly improve the text.

My dear family, Danica, Zoran and Alen, thank you for all of your love and support, both up close and at a distance.

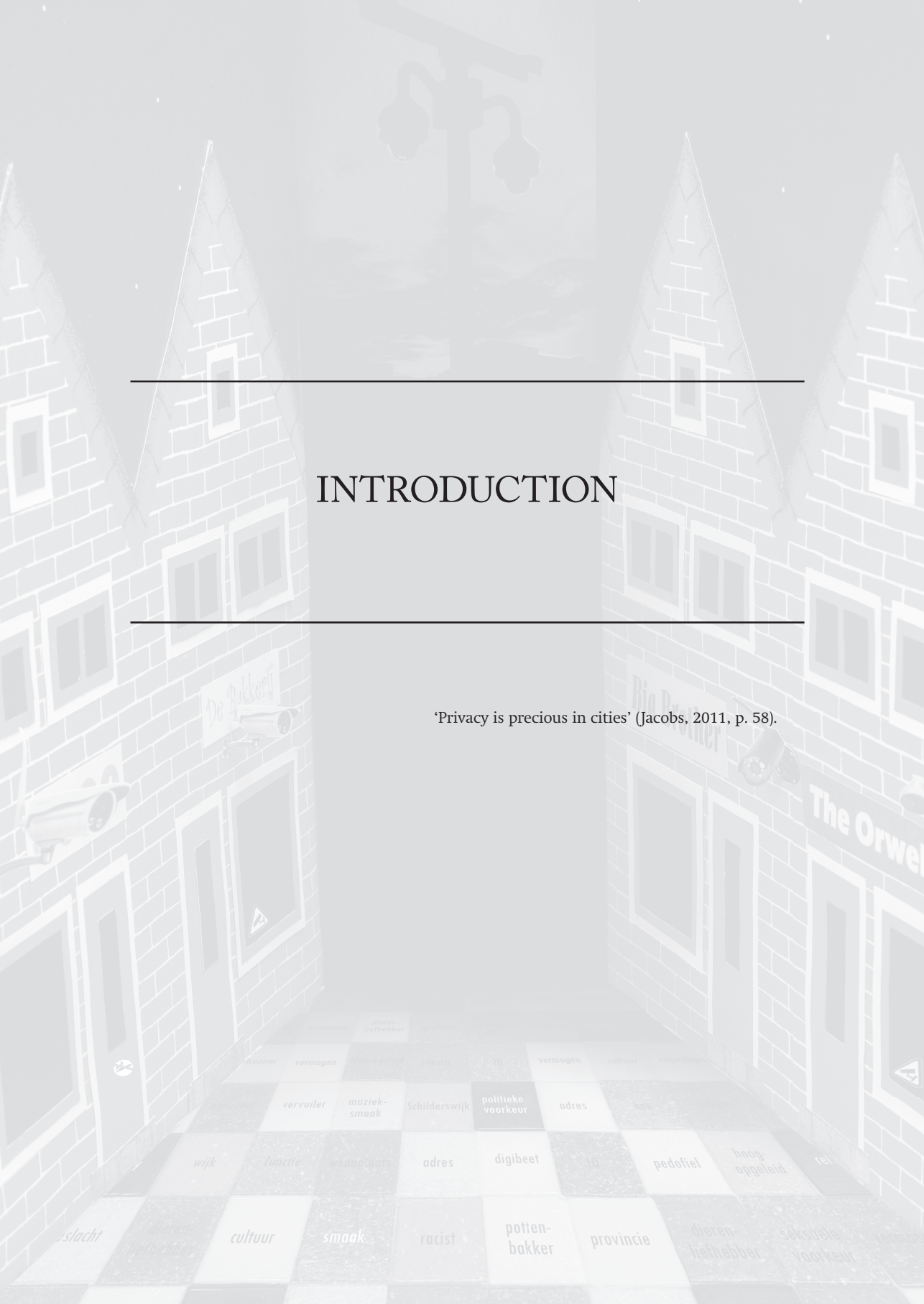
And last but not least, I would like to thank Aleš, without whom none of this would have been possible.

LIST OF ABBREVIATIONS

APV – Algemene Plaatselijke Verordering (Dutch General Municipal Ordinance)
ASBO – anti-social behaviour order
BID – business and innovation district
CCTV – closed-circuit television (video surveillance)
DPA – Data Protection Authority
ECHR – European Convention on Human Rights
ECmHR – European Commission of Human Rights
ECtHR – European Court of Human Rights
EU – European Union
GDPR – General Data Protection Regulation
GPS – Global Positioning System
ICT – information and communication technology
LEAs – law enforcement agencies
LGBTQ+ – Lesbian Gay Bisexual Transgender Queer/Questioning
NGO – non-governmental organisation
PiP – privacy in public space
PfP – privacy for public space
POPs – privately owned public spaces
PPP – public private partnership
PSPO – public space protection order
RFID – radio-frequency identification
SIA – surveillance impact assessment
SLL – Stratumseind Living Lab
SOAPs – stay out of areas of prostitution
SODAs – stay out of drugs areas
UDHR – Universal Declaration of Human Rights
UK – United Kingdom
U.S. – United States of America

INTRODUCTION

‘Privacy is precious in cities’ (Jacobs, 2011, p. 58).



1. BACKGROUND

Smart city and living lab initiatives, generally referring to the extensive embedding of software-enabled technologies into urban environments, are a common sight in cities around the world by now. They seem an almost obligatory feature of any city (or town) in the developed world, including in Europe, where the European Commission incentivises such projects through substantial funding opportunities.[1] The Netherlands is no exception and can be described as a country fully committed to smart city and living lab projects.[2] It is thus becoming increasingly difficult to walk the streets of a Dutch city (large or small) without being monitored, tracked and sometimes acted upon through a variety of sophisticated digital technologies. In Eindhoven, for instance, we find sound sensors and video cameras with embedded capabilities (including people counting, detection of mood and walking patterns) for the purpose of detection of 'escalated' behaviour and alerting the police, as well as lamp-posts fitted with special lighting technology intended to affect the mood of passers-by.[3] In Enschede, traffic sensors register the unique identification numbers of persons' smartphones in order to see how often people visit the city and what their routes and preferred spots are. The municipality also launched a 'smart traffic' app that rewards people for 'good behaviour' like cycling, walking and using public transportation instead of driving (ironically, one of the rewards is a free day of private parking in the city).[4] The app, however, also creates 'personal mobility profiles' and the collected data belongs to the private company offering the technology. Some cities, including Utrecht, keep track of the number of young people hanging out in the streets, their age group, whether they know each other, whether or not they cause a nuisance, and the 'atmosphere' on the street (Naafs, 2018). Law enforcement keeps track of this information through mobile devices, calling the process 'targeted and innovative supervision' (*ibid.*). There is also mention of predicting school drop-outs, poverty and the monitoring of the health of certain groups with the aim of intervening more expeditiously (Naafs, 2018).

1 See, for instance: European Commission. (n.d.). Smart cities. Retrieved March 19, 2019, from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en; EIP-SCC. (n.d.). The European Innovation Partnership on Smart Cities and Communities (EIP-SCC). Retrieved March 19, 2019, from https://eu-smartcities.eu/.

2 See NL smart city strategy: the future of living. (2017). Retrieved March 19, 2019, from https://instituteforfutureofliving.org/wp-content/uploads/NL_Smart_City_Strategie_EN_LR.pdf.

3 There is no official website for this project, called the Stratumseind Living Lab. See, for instance: van Dijk, M. (2018). Stratumseind: de datastraat van Eindhoven. Retrieved from https://innovationorigins.com/nl/stratumseind-de-datastraat-van-eindhoven/.

4 See Enschede (gemeente). (n.d.). SMART: Self-Motivated And Rewarded Travelling. Retrieved March 19, 2019, from https://www.smartintwente.nl/over-smart.

The *make-up* of public space has been changing particularly since the 1990s, when urban public space came to be increasingly sentient through sensors and other surveillance technologies, such as smart CCTV, wifi, cellular networks and automated number plate recognition (Timan, Newell, & Koops, 2017a). In general, surveillance can be about both caring and controlling (Lyon, 2006). The subject of surveillance is being watched with a certain purpose, which can be controlling and disciplining the subject into certain behaviour or a set of norms, but also – possibly at the same time – protecting and caring for that subject (Galič, Timan, & Koops, 2017, p. 10). The introduction of CCTV into city centres, for example, was done in the name of crime prevention and persons' safety more generally. The proliferation of surveillance in public space is, thus, not limited to the smart city or living lab development. However, such initiatives – with relentlessly positive promises of efficiency, safety and sustainability – have greatly advanced the deployment of such technologies in urban public space. People in urban public spaces today – *everyone* who is present in public space – are thus subject to levels of intensified scrutiny, as increased aspects of their daily lives are captured as data (Kitchin, 2016). While surveillance in itself is neither good nor bad (connected to its possible goal of both caring and controlling), it is also not neutral (cf. Kranzberg, 1986). This is a judgment value, which is very much dependent on the context and the manner in which surveillance is deployed. Given the scale and often brash application within smart cities and living labs today, it is important to scrutinise the non-neutral application of surveillance. In other words, there is a 'mass public surveillance problem' (Froomkin, 2017, p. 1738) in contemporary smart cities and living labs, one that keeps on growing as cities amass ever more surveillance technologies.

Such pervasive surveillance that is, at least generally, applied to everyone and in all contexts – all places, times, networks and groups of people (Marx, 2002) – is diminishing our sense of and experience of privacy in public space. This spread of surveillance, at least in the Western world, generally follows from the vague idea that there is no privacy in public space, nor should it be. This idea is based on a traditional understanding of the binary distinction between public and private (referring to spheres of society, a broad concept including physical space and other ways in which society is organised), understood as exclusionary opposites (Bobbio, 1989, p. 1). This means that what is private cannot be public and *vice versa*. Moreover, from such a perspective the public sphere is understood as a domain of visibility, so that entering the public domain (including public space) means accepting to become a subject of visibility. From this perspective, the notion of privacy in public space thus sounds like a conceptual miscarriage, and surveillance of public space can hence be seen as *the natural order of things* (Brighenti, 2010b). However, the public/private distinction is not

a natural division, it is rather a powerful ideological tool (Cutler, 1997). Public and private are contested realms, heavily debated in various (sub)disciplines, including human geography, political theory and feminist studies. In practice, the distinction seems more fluid than the binary opposition suggests, as people live in much more complicated, fluid and hybrid worlds (Blomley, 2005). After all, we live large and important parts of our private lives in public space. We read in the park, we kiss our partner in alleys and we stroll the streets. In fact, people have been enjoying a fair level of privacy in public space in practice, largely as a result of practical obscurity, inconspicuousness and reserve (e.g. Westin, 1967). Or as Donath (2014, p. 302) put it:

> 'Walking down a street today, I can see many people – strangers – going about their business. Although we are all out in public together, we retain quite a bit of privacy. I do not know where they are going or why, nor do I know much about them beyond what they have chosen to reveal about themselves. Our privacy [in public space] comes not from being hidden, but from being obscure. … Our unaugmented public display, while not entirely uninformative, provides a layer of privacy through vagueness, ambiguity and the ease of imitation.'

This layer of obscurity is enhanced by our attitude towards others in public space, whom we treat with reserve – voluntarily limiting our curiosity and knowledge about them as we interact with them in a wide variety of social roles. People therefore experience privacy, at least to a certain extent, not only behind closed doors and drawn curtains, but also in those parts of our lives that are lived out in public and dispersed over space and time (Reiman, 1995, p. 29). It is thus more appropriate to see the relationship between private and public as very much connected, even interdependent, where private and public exist among shades of privateness and publicness (Madanipour, 2003, p. 107). Public and private spaces are thus essentially layered spaces. An illustrative example of such layeredness in public space, on the one hand, can be found in the public toilets positioned in clear view in the streets, often offering only a thin layer of privacy (through some sort of architectural design) that requires a fair level of reserve in order to be truly achieved. Public spaces should thus be thought of both as spaces of exposure and visibility as well as spaces of obscurity and reserve. At the other side of the private/public divide, an example of such layeredness in private space can be found in the distinction between different rooms in a person's home, where some are more public than others – guests are usually invited into the living room, a more public part of the home, whereas the bedroom is considered off limits.

The rapid technological developments that have permeated all parts of our lives are diminishing the possibility of enjoying a more or less desirable level of privacy in public space. On the one hand, increasing aspects of our private lives are spilling over into public space, especially through smartphones and other computing devices that commonly contain large amounts of private data that we carry with us as we move in and through public spaces every day. On the other hand, an increasing level of digital technologies embedded in the physical environment of our cities is monitoring ever more parts of our lives in public (also by communicating with our own computing devices) and thus breaking down the 'reliable solidness of built space' (Nissenbaum & Varnelis, 2012, p. 10). Public spaces are thus no longer layered spaces of exposure *and* obscurity; instead, they are becoming spaces of *hyper-exposure*. People can no longer count on behavioural, temporal and spatial considerations through which they produced and maintained some kind of boundary and distance from others – in other words, privacy in public. We have become increasingly *transparent* or *hyper-visible*, as even the most private parts of our life, our thoughts and emotions, can now be detected – or so it is claimed and attempted – via the measurement of sweat, heart-rate and retina changes (Davies, 2015).[5] Whereas visibility can result in empowerment leading to recognition (Honneth, 1995), hyper-visibility in the contemporary smart city or living lab can also result in disempowerment, ever tightening social control and other issues that are related to the broad concept of privacy as boundary management (Altman, 1975).

If the problem of privacy in public space did not exist in any compelling form in practice in the recent past (Nissenbaum, 1998, p. 574), it has now certainly become a serious issue.

I submit that the topic of privacy in public space is of particular academic importance today, since it has not received sufficient attention for three main reasons. First, in contrast to privacy in general, privacy in public space has not been the focus of intense scholarly debate for the past hundred years (even if some of the debate on privacy in general has resulted in serious disagreement). While 'public privacy' was introduced already by Westin in his seminal 1967 book, *Privacy and Freedom*, the topic of privacy in public space only came to somewhat broader scholarly attention in the late 1990s (see

5 See, for example: Handeyside, H. (2015). Be careful with your face at airports. Retrieved March 19, 2019, from https://edition.cnn.com/2015/03/19/opinions/handeyside-tsa-spot-program/index.html; Privacy International. (2017). Biometrics knows no borders, it must be subject to extreme vetting. Retrieved March 19, 2019, from https://medium.com/@privacyint/biometrics-knows-no-borders-it-must-be-subject-to-extreme-vetting-b13bf6420253.

Nissenbaum, 1997, 1998). Still, the topic has remained at the outskirts of academic interest, at least until today.[6] As such, it is also under-researched, lacking insight into the contemporary relationship between private and public, and the particular values and roles of privacy in public space, both for individuals as well as for society in general.

Second, privacy in public space has hardly been the object of legal regulation. Although there have relatively recently been a few influential judgments acknowledging a certain level of privacy in public space, both in Europe (see Chapter 6) and the U.S.,[7] laws generally still largely rely on a rather stiff division between private and public spaces when it comes to protecting privacy. Consequently, many or most aspects of our lives in public fall out of the scope of classical privacy protection. Moreover, surveillance in public space that is performed by private actors, often in cooperation with public actors in some form of a public-private partnership (as is commonly the case in smart cities), is hardly regulated at all, at least in Europe (I discuss this briefly in Chapter 7).

Finally, the deployment of ever more sophisticated information and communication technologies (ICTs) in public space, combined with the lack of scholarly attention and legal regulation, is rendering opportunities for privacy in public space incredibly scarce. This context contributes to making the notion of privacy in public seemingly a non-issue, or even a lost cause. It should come as no surprise then, that in such conditions many data analytics and other technology companies (including big businesses like Microsoft, Cisco, Siemens, IBM, and Intel) are now pursuing business models that largely rely on actively capturing data from the physical world, rather than using data provided by others or capturing them online (Kaminski, 2015, p. 1121). As Kaminski (2015, p. 1121) put it, this brings us – and especially legislators – back to the (older) question of how to govern surveillance that takes place in the physical world (rather than focusing solely on the online world).

In this dissertation, I aim to remedy the neglect for privacy in public as outlined above. I thus address the need for academic research on the values and roles of privacy in

6 Recently, two edited books on the topic of privacy in public space have been published, signalling a larger interest in the topic. See, for instance, (Newell et al., 2019; Timan, Newell, et al., 2017b).

7 In Europe, this holds most notably for the case law of the European Court of Human Rights, which I examine in Chapter 6. In the U.S., this can be seen in the following judgments: *Carpenter v. United States*, 138 S. Ct. 2206 (2018), *Riley v. California*, 134 S. Ct. 2473 (2014) and *United States v. Jones*, 565 U.S. 400 (2012), particularly judge Sotomayor's concurrence.

physical public space, the impact of digital surveillance technologies on it and the gaps in legal regulatory mechanisms for the protection of this manifestation of privacy, with a particular focus on Europe. I do so by examining the complex and multi-dimensional topic of privacy in public space in contemporary smart cities and living labs in a wide and in-depth manner through interdisciplinary research, analysing literature not only from law and privacy scholarship but also from surveillance studies, urban geography and political theory. Furthermore, I do so not only through theoretical research but also through an analysis of a living lab in practice – the *Stratumseind Living Lab* in Eindhoven, the Netherlands.

2. RESEARCH OBJECTIVES AND RESEARCH QUESTIONS

In view of the above considerations, I posit that there is a need for additional and in-depth conceptual reasoning that can then inform and guide a different legal decision-making that would allow for, in fact encourage, the protection of privacy in public space. My main aim, as a legal scholar, is to inform and convince other legal scholars and thus, indirectly, law-makers (and regulators more broadly) of the need for (additional) legal protection of privacy in public space. However, I also think the dissertation will be of value for non-legal scholars, particularly in relation to the complex intersections between other scholarly disciplines and law.

Against this background, I am addressing the main research question of this dissertation: *how can and should we conceptualise privacy in public space, especially within the context of surveillance in smart cities and living labs?*

In order to answer this broad question, several research sub-questions need to be answered. I have divided these and the dissertation itself in two main parts. The first part examines the 'foundational notions' of this dissertation – that is, privacy, surveillance, public space and smart cities and living labs. Since privacy in public space is a complex and layered topic, one must first understand the meanings behind the several complex notions involved before one can offer an answer to the main research question. The second part of the dissertation attempts to combine the insights from these various fields, resulting in a type of synthesis that is greater than the sum of its parts.

The first part thus involves the following set of sub-questions. First, I ask (1) how should we think of smart city and living lab initiatives (at least those in the West)

and what challenges do they pose, especially in relation to privacy? Since my study uses an example of a living lab in the Netherlands in order to ground the theory in practice, thus making it more illustrative, the following sub-question is, (2) how does the practical example of a living lab in the Netherlands – the *Stratumseind Living Lab* (*SLL*), inform these theoretical insights? Thirdly, I explore (3) how is surveillance conceptualised in prominent literature, particularly in surveillance studies? Furthermore, I ask (4) how is privacy – both as a phenomenon, concept and as a set of legal rights – conceptualised in general, especially in Europe? I pose this question in order to later determine, whether these generally identified values, dimensions and mechanisms of privacy broadly fit, warrant and enable the protection of privacy in public space or whether other conceptualisations should be created. And, finally, (5) how is public space conceptualised in prominent literature (primarily in urban geography and political theory) and what are the key interests and rights connected to public space?

The second part of the dissertation brings insights from these very different fields of scholarship together. In particular, I show how these foundational notions are articulated in different contexts: first, in the context of the *SLL* example and, second, in the legal context. Firstly, I thus examine (6) what types and characteristics of surveillance can be discerned from the *SLL* example and what kinds of privacy-related risks do they pose? Secondly, I examine (7) whether the right to respect for private life in Article 8 of the European Convention on Human Rights (ECHR) protects privacy in public and, if so, based on what reasoning and to what extent? Based on insights from all of the previous chapters, I then explore (8) how privacy in public space within contemporary smart cities and living labs could and should be conceptualised? An answer to the main research question – that is, a possible way of conceptualising privacy in public space – can offer insight into legal regulation of pervasive surveillance in public spaces as is taking place within contemporary smart cities and living labs. However, as is usually the case with very complex matters, they do not render themselves *reducible* to simple and uniform solutions. Therefore, I end this study by briefly looking into (9) how surveillance within smart cities and living labs could be regulated (going beyond the law) in order to address the various types of privacy-related risks stemming from it?

This dissertation thus aims to be largely theoretical, with limited aspirations of practical utility. In order to offer any sort of meaningful suggestions for the regulation of surveillance in public space within smart cities/living labs, this study requires a narrowing down of focus in terms of jurisdiction. Given that both the practical example of the *Stratumseind Living Lab* and the European Court of Human Rights (ECtHR) case law that I examine stem from Europe, it makes sense to limit the focus of the research

to Europe, in particular to continental legal systems (which the Netherlands belongs to). Nevertheless, theoretical insights, particularly in relation to the foundational concepts stemming from other jurisdictions, especially the United States of America (U.S.), which has a leading role in the field of privacy scholarship (see e.g. Brandeis & Warren, 1890; Westin, 1967), will be thoroughly analysed.

3. METHODOLOGY

3.1 Interdisciplinarity

It can be easily observed from the introductory paragraphs above that privacy in public space is a topic that transgresses the boundaries of many academic disciplines and sub-disciplines. It concerns issues of urban public space and its regulation, therefore, involving the disciplines of urban geography and political theory. It is also essentially about surveillance of public space and as such demands an analysis from the perspective of surveillance studies. Then, of course, it is about privacy. Privacy scholarship itself is largely based on philosophical, psychological and sociological research. Moreover, when complemented with legal research, especially human rights law, it leads to insights into the right to privacy (and the right to data protection). Surely, the topic of privacy in public space touches upon issues from yet other academic (sub)disciplines, for instance security studies, responsible innovation and urban design. However, one cannot study all disciplines here, and I have settled on the above set of disciplines, which I consider adequate to provide a sufficiently broad and deep overview of the complex, boundary-crossing topic of surveillance in physical public space (rather than the online environment) and its legal regulation. While the regulation of online space (or cyberspace) is at least as important as the regulation of physical space, this study focuses on the physical spaces of living labs and smart cities, which have been largely neglected in scholarly literature, including legal scholarship. Nevertheless, since through the embeddedness of digital technology, physical public spaces become endowed with digital characteristics, transforming into 'code/space' (Kitchin & Dodge, 2011), I will also partially engage with this aspect of public space (see Chapter 4).

One noteworthy limitation of this study is its exclusion of research into data protection law. The main reason for this is that, while data protection scholarship seems to be in full bloom (especially in Europe in view of the coming into force of the General Data Protection Regulation in May 2018), privacy scholarship is receiving far less attention. Moreover, given the chosen focus of this dissertation – the conceptualisation (and regulation) of privacy in physical public space – a broader focus going beyond the informational aspect of privacy (strongly connected to data protection) is needed.

While an individual's control over data produced about her is a necessary condition for the protection of privacy (and, furthermore, the values that privacy serves), it is not sufficient (cf. Rouvroy & Poullet, 2009, p. 51). Therefore, in this study I focus on non-informational types of privacy, particularly associational, behavioural and spatial privacy. Of course, as noted in *A typology of privacy* (Koops et al., 2017, pp. 568–569), informational (or data) privacy is an overarching aspect of all other types of privacy, as each type of privacy contains an informational element – that is, a privacy interest exists in restricting access of controlling the use of information about that particular aspect of human life. For instance, bodily privacy is not limited to restricting physical access to the body, but also to restricting and controlling information about the body, such as health or genetic information. In this sense, while this dissertation does not engage with data protection law, it does not negate the importance of the informational aspect of privacy.

The broad objective of the study comes with both pleasures and pains. It poses numerous challenges to me, as a scholar primarily educated in law. I need to discover – for the first time – these various fields that cross the topic at hand. In order to gather insights from these diverse disciplines, I need to engage in a dialogue with them – their theories, concepts and sometimes even their methods. As such, privacy in public space is an interdisciplinary problem that demands examination relationally through dialogue between these different disciplines and fields (Barry et al., 2008, p. 30). In fact, interdisciplinary research is surprisingly fitting to the topic of privacy in general (and privacy in public space in specific), which is very much about preserving and transgressing boundaries. This dissertation alike is thoroughly interdisciplinary – in it I integrate knowledge and perspectives from the mentioned (sub)disciplines, using a synthesis of approaches. I view this research as interdisciplinary rather than multidisciplinary, as it shows a commitment to bring different disciplines together and attempts to integrate (or translate) the contributions of these disciplines and sub-disciplines (Barry et al., 2008; Lawrence & Despres, 2004).

While all of these (sub)disciplines critically discuss issues connected to privacy in public space, only rarely do they do this directly. The key goal in this dissertation therefore is to gather the insights from these various disciplines in order to connect and integrate them, leading to a conceptualisation of privacy in public space, and convincing legal and privacy scholarship of its need and value. This is connected to the more specific goal of advancing privacy scholarship through the integration of insights from urban geography and political theory, disciplines that have not been traditionally used for this purpose. Furthermore, it connects to my general attempt to apply – as much as possible – the insights from the above disciplines into legal

scholarship. I write 'attempt' because such an integration and translation are not at all easy tasks. A part of the aim of interdisciplinary research itself is to expose friction from the interaction of various fields of research (Barry et al., 2008, p. 26). Contrary to some claims, interdisciplinary integration does not bring independent parts of knowledge from different disciplines into 'harmonious relationships' via synthesis (Stember, 1991, p. 4). Such friction exists already within disciplines (Barry et al., 2008; Laclau & Mouffe, 2014). I have encountered this within my own discipline of law, finding that it is very difficult to communicate between privacy law scholars (often rooted in general privacy scholarship and fundamental and human rights law) and data protection law scholars (rooted mostly or entirely in informational or data privacy theory and European data protection law). But the friction is clearly exacerbated when different fields are combined.

As a primarily legal scholar, I am aware that I require *chutzpah* – gall, audacity, insolence – to enter these demanding and unknown areas of research. As Seligmann (2014, p. 11) put it, '[i]n its original Hebrew usage, *chutzpah* was viewed negatively as a quality attributed to someone who has overstepped the boundaries of accepted behaviour.' There is a double *unacceptability* at play in this dissertation. On the one hand, from the perspective of legal scholarship, my endeavour in this study can be considered unacceptable, since it dives so much into other academic disciplines that it renders the research hardly legal in the end. And, on the other hand, from the perspective of disciplines other than law into which I venture, the dissertation can be considered unacceptable because it likely lacks a certain knowledge, a widely accepted reservation or a nuance, that would be present in the work had the job been done by an *insider*. And yet, this is what lies at the heart of interdisciplinary research, where one situates oneself in the many academic (and cultural) contexts with which they are unfamiliar. Interdisciplinary research, as I have undertaken it, calls for *chutzpah*.

The overarching goal of this research is thus to advance the understanding of privacy in public space in ways that would not have been possible through mono-disciplinary or even multi-disciplinary means. This is in line with the final goal of this dissertation – to inform legal (privacy) scholars about the complexities of and the needs for preserving privacy in public space and, ideally, to convince law-makers of the need for further regulation that would introduce or strengthen such a right. And while legal scholarship is my ideal audience, I nevertheless hope that this study will reach a far broader audience that is interested in a broad yet sufficiently deep overview of the issue of surveillance in public space within smart cities in an attempt of a conceptualisation of privacy in public space.

3.2 'Going native'

The manner in which I engage with the different disciplines and sub-disciplines, namely urban geography, political theory, surveillance studies and privacy scholarship (as rooted in philosophy, psychology, sociology and law), I refer to as 'going native'.

'Going native' is a key concept in ethnography, and generally refers to the danger of becoming too involved in the community under study, thus losing objectivity and distance – in simpler terms, getting too close (O'Reilly, 2009). It is thus sometimes used as a derogatory term in ethnography,[8] referring to the tendency of some ethnographers to forget that they are conducting research and are becoming full-fledged members of the community under study, thus, perhaps never 'going [back] home'; in other words, suffering from *oikophobia*.[9] Of course, as I am not conducting any sort of ethnographic research, I am using the term 'going native' in a metaphoric sense of fully emerging into a particular discipline by adopting the particular language as well as some of the accompanying biases of the discipline in question. For instance, there seems to be a persistent bias in surveillance studies to overemphasise the risks of surveillance (seeing surveillance as bad, bad, bad!) and to overlook its possible positive aspects (connected to care). A similar bias is found in large parts of urban geography and some political theory scholarship, where the loss of 'public space' is lamented and smart city or living lab initiatives are conceived in almost only negative terms. Some of this bias has certainly been *transplanted* into my own Chapters. This is one of the risks of 'going native'. The metaphor of suffering from *oikophobia* seems suitable for my research, which is about public space, commonly considered the antithesis of the home. However, the main idea for my going native in the first place, is to finally go back home; that is, to gather insights from various fields and 'translate' them into insights at least partially comprehensible to the legal scholar and, ideally, the law-maker or regulator more broadly.

The disciplines and sub-disciplines that I am dealing with in this study are considered either social sciences or humanities, as they are in some way concerned with society, culture and the relationships among individuals within a society. Furthermore, they can also be described as critical studies – they are orientated toward normative questions, particularly those involving some form of oppression, understood in a broad

8 Although nowadays rather associated with the language and attitudes of colonial ethnography (O'Reilly, 2009).

9 My use of this term is in no way connected to the politically loaded way that Thierry Baudet has been using it in contemporary Dutch politics.

way.[10] This dissertation mainly offers theoretical analyses of literature from several disciplines connected to the contemporary phenomenon of surveillance within smart cities and living labs and its effect on our privacy and the rights to privacy in public space. This effect on privacy is here understood as a potential type of oppression, albeit non-physical in nature. In line with the approach in critical theory, this study does not stop at the level of description but makes substantiated (although sometimes perhaps a bit *natively* biased) normative claims about this – for instance that such surveillance carries many inherent risks or that a fair level of privacy is desired also in public space, both from an individual and from a societal perspective.

A smaller part of this study, in particular those parts dealing with Article 8 ECHR case law (Chapter 6), is conducted through doctrinal legal research, that is the research process used to identify, analyse and synthesize the content of law (Hutchinson, 2017). I do not presuppose that an identifiable content of law exists in advance, rather, I research and interpret the law based on its interpretation and application by courts (most notably the ECtHR) and other legal scholars.

Due to this varied approach to my study, several styles of writing and language are found in the chapters. The shape of this study can thus be described as kaleidoscopic – offering multiple perspectives on the same matter, in this case privacy in public space in contemporary smart cities and living labs. This seems fitting to the topic at hand, as the right to privacy itself has been described as kaleidoscopic: '[m]odify the angle of observation, and its physiognomy is altered as if it were not exactly the same right in each position' (Picard, 1999, p. 58). I am aware that some of these chapters, especially since most of them are highly theoretical, will be demanding to read, particularly for legal scholars. For this reason, I have provided each chapter with a brief conclusion written in a language that is as clear and plain as possible, capturing the main points relevant for the main goals of this dissertation. Furthermore, as some of these chapters correspond to a particular academic discipline, I have written them in such a way that they both inform the dissertation from that particular point of view as well as stand on their own. As such, they sometimes offer additional information on certain topics that I discuss from the specific discipline that I examine. For instance, the first chapter on smart cities and living labs offers a brief overview of the various critiques of such initiatives, particularly from the perspective of urban geography, not all of which are necessary for the topic at hand. Nevertheless, they are informative for the inquisitive

10 See Bohman, J. (2005). Critical Theory (Stanford Encyclopedia of Philosophy). Retrieved March 19, 2019, from https://plato.stanford.edu/entries/critical-theory/.

reader, offering a broader perspective on the complexity of topics at hand, and thus also intended to offer fruitful ground for further enquiry in future scholarship.

3.3 The *Stratumseind Living Lab* example

Alongside theoretical desk research, this dissertation is also informed by a practical example of a living lab connected to smart city development in Eindhoven, the Netherlands – the *Stratumseind Living Lab*. This is particularly valuable since the topic of my dissertation – privacy in public space – is a highly relevant topic due to the contemporary phenomenon of pervasive surveillance in public spaces within smart cities and living labs. It thus makes sense to examine a practical example of such a phenomenon in Europe, which is the focus of my study. In Chapter 1, I thus describe and analyse the dissemination and operation of the living lab/smart city concept as presented in the example of the *Stratumseind Living Lab* (*SLL* or *Living Lab*), in order to test and further guide the insights on surveillance and privacy in public space gathered from theoretical research.

The *SLL* was chosen as a valuable and insightful practical example of a living lab connected to a smart city due to several reasons. The first reason is its longer-term existence. The *SLL* officially operated during mid-2013 and mid-2018 (unofficially, it seems to still be operating today),[11] with many interesting activities and results to be studied. The second reason relates to the involvement of major international businesses in the field of information and communication technology (ICT) in the project, including Atos, IBM, Intel, Cisco and Philips (alongside smaller local companies). Furthermore, the key public entity of this public-private partnership is the Eindhoven municipality, which is one of the biggest Dutch municipalities and has been elected the 'smartest region in the world' in 2011 by the Intelligent Community Forum,[12] promoting itself as a global hotbed for (social) innovation. Third, the diversity of the projects connected to the *SLL*, with an explicit focus on both safety and profitability, makes it an interesting example to study, enabling the discovery of diverse insights. In this sense, I do not claim that the example chosen is typical of living labs (or smart cities) in general; rather, I claim that it is symptomatic (Born, 2009), meaning that it can serve as an 'anchor point' to identify central issues that

11 See Stratumseind Living Lab. (2019). Living Lab, Stratumseind 2.0. Retrieved March 19, 2019, from https://www.facebook.com/LivingLabStratumseind/, showing a picture of Vinotion's 'ViSense CrowdDynamics' technology (with an upgrade) posted on 18 February 2019 and referring to further work within the *SLL*.

12 See European Commission. (2011). Brainport region is the "smartest region of the world." Retrieved March 19, 2019, from https://ec.europa.eu/digital-single-market/en/news/brainport-region-smartest-region-world.

demand specific attention and analysis in relation to privacy in public space within European living labs and smart cities. Finally, this example is chosen because it is a part of the author's doctorate research,[13] which required research into privacy issues specifically connected to the *SLL*, enabling greater access to the actors, activities and documents taking place within the *SLL* that are otherwise usually inaccessible to the general public.

In this dissertation, I have decided not to conduct a proper case study – that is, an up-close, in-depth, and detailed examination of a specific case and its related contextual conditions – but to use the *SLL* as an illustrative example in a looser fashion. I have done so due to reservations about my own skills as a lawyer to conduct proper qualitative research in social science, as well as due to the need of limiting the scope of my study, which was already very broad. This is thus a limitation of this part of my research, in that it cannot offer a completely reliable result that contributes to the theory of living labs or surveillance as such. Instead, the *SLL* example is used to serve as an insightful and illustrative example that makes the rather abstract claims of surveillance and the promises and perils of smart cities come to life.

I have based my description of the *SLL* on research that took place between 2014 and 2018 and consisted of critical analysis of policy documents, promotional literature and newspaper coverage related to the *SLL*, information gathered at meetings and via email as well as some qualitative interviews with the parties involved in implementing the *SLL*, in particular with representatives from Eindhoven municipality, the Technical University in Eindhoven, the Dutch Institute for Technology, Safety and Security (DITSS), Sorama and Vinotion (local technology companies) and Atos Nederland.

While I did conduct three 'qualitative' interviews – that is, two unstructured and one semi-structured interview – with several of the *SLL* parties,[14] most of my insights stem from analysis of information gathered through policy documents, email exchanges and informal conversations. Of course, unstructured interviews are very much like informal conversations, where going off topic and asking follow-up questions is encouraged (Bryman, 2012, pp. 470–471; Burgess, 1984), so that it is difficult to

13 The author's PhD project was 50% funded by the Dutch Institute for Technology, Safety and Security (DITSS), which is an actor within the *SLL*.

14 I conducted the interviews on the following days: 23 October 2014, 31 August 2015 and 13 April 2016. Qualitative interviewing is seen as flexible, responding to the direction in which interviewees take the interview. This flexibility allows the researcher to adjust the emphases in her research as a result of significant issues that emerge in the course of interviews (Bryman, 2012, p. 470).

distinguish between them. Most notably, I conducted a semi-structured interview in May 2017 with Tinus Kanters, a representative from Eindhoven municipality, and Peter van der Crommert from DITSS. Both were involved in all of the sub-projects of the *Living Lab*, so they had a good overview of what was taking place and were, as such, good persons to interview. In this interview, I had an 'interview guide' – a list of question or fairly specific topics that I wanted to address (Bryman, 2012, pp. 472–473). Nevertheless, even in this form of interview I gave the interviewees great leeway in their replies, the order of questions that I posed sometimes differed from the guide and I also asked follow-up questions. In conducting these interviews, I was mostly interested in gathering as much factual information about the types of information and communication technologies and their capabilities within the *SLL*.

I was thus not particularly interested in the particular *way* my interviewees stated certain things but more in the *what* they said. This differs from qualitative interviewing, in which the interviewer is also interested in how the interviewees frame and understand the relevant issues and what they thought of as important in explaining and understanding these matters (*ibid*., p. 471). Because of this, I also did not record and transcribe my interviews (which might have also made my interviewees feel uncomfortable and reveal less or less accurate information), I only made notes during and immediately after the interviews. As such, these unstructured and semi-structured interviews, might better be classified as informal conversations.

As mentioned, most of my insights into the operation of the *SLL* stem from an analysis of information gathered from official documents, mission statements, emails, conversations with the parties and news-coverage on the *Living Lab*. Some of this information originates from the parties of the *SLL* themselves (either the municipality or private companies) at request of the researcher, and some was found available to the public on the internet. Since the aim of this practical part of my research was to illustrate a type of living lab and surveillance of public space in practice, I did not fully examine these sources in terms of their authenticity, credibility, representativeness and meaning (Bryman, 2012, p. 544; Scott, 1990, p. 6). Nevertheless, I did examine the specific sources of data in the context of other sources, thus ironing out clear errors, inconsistencies and biases. I was particularly interested in a simple qualitative content analysis by gathering as much information as possible into *how* the *Living Lab* actually functions (or does not function), trying to find those elements of the initiative that would be most relevant for my subsequent analysis of privacy-related risks on the Stratumseind street. As such, the created representation of the *SLL*, like all analyses of documents, should not be regarded as providing an objective account of the state of affairs (Bryman, 2012, p. 551).

SLL actors that have shared textual sources and other information with me, have given me permission to use and publish most of the information that I have gathered in this way; the information regarding which they have not provided me with permission, I do not use in this dissertation.

4. STRUCTURE

Given the complexity and layeredness of the topic at hand, I have described the shape of this dissertation as kaleidoscopic – offering multiple perspectives on the same matter. As such, there is no clearly best structure of the study. As already mentioned, I have chosen to structure the dissertation in two main parts. The first part examines the 'foundational notions' (Chapters 1-4). Following a pragmatic philosophical approach, I have chosen to begin with a general discussion of smart cities and living labs and the example of the *Stratumseind Living Lab* in order to offer an illustrative example, to which one might apply the more abstract notions of privacy, surveillance and public space that follow. In Chapter 1, I thus set the stage for the research by examining notions of living labs and smart cities, both from a theoretical as well as from a practical perspective.

The first Chapter is followed by a chapter on surveillance theory, offering a very different perspective on the innovative projects calling themselves smart cities and living labs. Chapter 2 offers a rough chronological-thematic overview of surveillance concepts and theories in the form of three stages: panoptical, post-panoptical and contemporary piecemeal theories and concepts of surveillance. I have done so in order to provide a more structured insight into the various forms of surveillance and to show that choosing a surveillance framework through which to analyse a particular type and context of monitoring matters. An analysis of surveillance within the *SLL*, for example, through the lens of the prison Panopticon, surveillant assemblage or Foucault's security will shed a rather different light and thus different implications for human rights and community life.

As the concept of surveillance can be described in orthogonal relationship to privacy (J. E. Cohen, 2017, p. 458), the following Chapter examines privacy, both as a theoretical and legal concept, thus suggesting new criteria for analysing the effects of surveillance in smart cities and living labs. The aim of Chapter 3 is to identify the underlying values, types and mechanisms in privacy theory in order to inform the conceptualisation of privacy in public space. This will enable me to determine in the second part of this dissertation, whether these generally identified values, dimensions

and mechanisms of privacy broadly fit, warrant and enable the protection of privacy in public space or should other conceptualisations be created.

The last Chapter of the first part offers an exploration of public space as the remaining concept to be examined in the particular context at hand. In the particular context of privacy in public space, a key notion is commonly overlooked in the discussions of privacy scholarship – that is, the notion of public space. Therefore, the general aim of Chapter 4 is to unveil various aspects of urban public space that are particularly relevant for the subsequent conceptualisation of privacy in public space. The central focus here is on physical urban space of Western societies, with its particular political, social and psychological significance.

The second part of this dissertation brings these notions together, analysing their articulation in two particular contexts (Chapters 5-6). In Chapter 5, I apply surveillance and privacy theory to the *SLL* example, discerning the types and techniques of surveillance within the *SLL* (and similar initiatives focused on safety and profitability) and their privacy-related implications. The example of the *SLL*, however, comes with its own limitations. So as to go beyond the particularities of the *SLL* (and also in view of a lack of detailed information on its functioning), I employ short hypothetical scenarios, some more and others less speculative, in my discussion. These scenarios allow me to identify and analyse the privacy-related risks stemming from the *SLL* but going beyond the particular successes or failures of the *SLL*.

In Chapter 6, I examine the level of protection of the right to respect for private life in public, including the reasoning behind it, as stemming from ECtHR case law. I determine that the ECtHR, through a dynamic and broad reading of the right, grants a rather broad level of protection of privacy also in public space. Following the broad manner in which the Court employs three notable categories in its assessment, I examine the matter in a tripartite structure – distinguishing between space, activity and data. In the concluding part of this Chapter, I briefly examine the *SLL* through the lens of Article 8.

The second part ends with a concluding Chapter (Chapter 7) suggesting a conceptualisation of 'privacy *for* public space' and brief thoughts on regulation. In this concluding Chapter (as in the dissertation as a whole), my aim is to further the scholarship emphasising privacy's broader societal and political value, and to do this in the particular context of privacy in public space. The Chapter is structured in two parts. In the first part I offer a rough outline of my own conceptualisation of 'privacy for public space'. This conceptualisation is an attempt at synthesis – drawing together

key threads of discussion throughout this dissertation, combining perspectives of privacy and public space (and, to a certain extent, surveillance) in order to explore how privacy in public space can and should be conceptualised so as to also address the social and political significance of public places. In the second part of the Chapter, I briefly examine the possibilities for regulation of surveillance of public space within smart cities and living labs by looking at Morgan and Yeung's (2007) five types (or Cs) of regulation: Command, Competition, Consensus, Communication, and Code. The Chapter ends with a final conclusion of the dissertation, offering a brief recap of the main points and ideas.

The structure of this dissertation thus consists of seven substantive chapters alongside an Introduction, where the last substantive chapter also serves as a concluding chapter.


De Bakker
Big Brother
The Orwe
vervuiler
muziek-
smaak
Schilderswijk
politieke
voorkeur
adres
wijk
functie
adres
digibeet
pedofiel
hoog-
opgeleid
cultuur
smaak
racist
potten-
bakker
provincie

PART I

1

SMART CITIES AND LIVING LABS
The city as a test-bed and the example of the *Stratumseind Living Lab*

1. INTRODUCTION

Smart city and living lab initiatives are a common sight in cities around the world by now. In fact, they are becoming an almost obligatory feature of any city or town in the developed world, including Europe. The contemporary city is thus increasingly built of pervasive and ubiquitous computing and digitally instrumented devices that are being embedded into the 'fabric of urban environments' (Kitchin, 2014, p. 2). Such technologies include digital cameras, sound and other sensors, meters, special lighting or smell technology, iBeacons and wifi tracking technology. Within the smart city/living lab discourse – as spoken by businesses, local governments and even supra-national entities like the European Union (EU) – such technology is seen as a solution to all sorts of urban problems, from traffic congestion and high gas emissions to the rising need of economic competitiveness among cities. The continual generation of data by these technologies is said to provide detailed and real-time pictures of urban practices and infrastructures that can be managed, synched and apportioned in order to optimise economic, resource and political efficiency, while still enabling social, cultural and urban development (Gabrys, 2014). As Kitchin (2015b) aptly put it, smart cities promise to solve 'a fundamental conundrum of cities – how to reduce costs and create economic growth and resilience at the same time as producing sustainability and improving services, participation and quality of life – and to do so in commonsensical, pragmatic, neutral and apolitical ways.'

Beyond the grand promises of the smart city/living lab discourse, however, pervasive information and communication technologies (ICTs) re-articulate the urban experience through its data-driven surveillance practices. People are now subject to much greater levels of intensified scrutiny as increasing aspects of their daily lives are captured as data (Kitchin, 2016, p. 5).[15] Moreover, people are transformed into sensing nodes or, in other words, citizen sensors (Gabrys, 2014, p. 32). From this perspective, smart city and living lab initiatives have wider implications for city administrations and citizens, in particular, they are diminishing privacy in public space. However, there is a lack of legal interest in these topics in academic writing (Edwards, 2016, p. 1). As explained in the Introduction, this dissertation aims to partially fill this gap by exploring living lab and smart city initiatives through the perspective of surveillance and privacy (including the right to privacy), with a focus on Europe. This Chapter, in

15 In this sense, it is more appropriate to talk about *capta* (something captured) rather than *data* (referring to something [freely] given). Due to the prevalent use of data in scholarship, I will continue using this term, although I will refer to the capture (rather than collection) of data in relation to surveillance in public space.

which I unpack the concepts of smart cities and living labs from a critical perspective (particularly from the perspective of urban geography), sets the scene.

In this Chapter, as in the dissertation in general, I do not contend that we need to abandon the creation of smart cities and living labs. Following Kitchin (2016), I submit that such initiatives need to be imagined and framed within critical discourses, including disciplines discussing public space, surveillance and (the right to) privacy. Framing, an important concept in a variety of academic fields, tells us that a particular framing of an issue involves social construction of phenomena, encourages certain interpretations, discourages or obfuscates others, and, consequently, invites a certain kind of criticism (Chong & Druckman, 2007; Van Gorp, 2007). In this Chapter, I frame living lab and smart city initiatives from the discourse of urban geography, which seeks to reveal their instrumental rationality and epistemology, to the extent relevant for the topic of surveillance of and privacy in public. Furthermore, I also examine a living lab initiative in practice connected to a smart city in becoming – the *Stratumseind Living Lab* (*SLL*) in Eindhoven, the Netherlands. It is, namely, important to study living labs and smart city projects in context, examining their particular implementation and functioning, as their assessment necessarily depends on how the concept is actually assembled, developed, filled with meaning and implemented by policy-makers (Vanolo, 2014, p. 884).

This Chapter therefore answers two sub-questions. First, *how should we think of smart city and living lab initiatives (at least those in the West) and what challenges do they pose, especially in relation to privacy?* And, second, *how does the practical example of a living lab in the Netherlands – the Stratumseind Living Lab (SLL), inform these theoretical insights?*

The structure of the Chapter is the following. I will first unpack the fuzzy concepts of smart cities and living labs by analysing literature from various academic fields, particularly from urban geography and technology and innovation studies. Following this theoretical discussion, I will present a detailed practical example of a living lab in the Netherlands – the *Stratumseind Living Lab* in Eindhoven. I will focus on three of its sub-projects, in order to reveal the discursive and material realities of 'actually existing' (Brenner & Theodore, 2002; Shelton, Zook, & Wiig, 2015) living labs and smart cities, at least in the Netherlands. Finally, in the last section, I offer a brief critical analysis of the concepts of living labs and smart cities and the *Stratumseind Living Lab* example, outlining key issues and challenges of smart cities and living labs as identified by urban geographers. As such, I will set the foundation for an in depth discussion of surveillance and privacy issues of living labs and smart cities and their regulation in the following chapters.

2. SMART CITIES, SMART EVERYTHING

The word 'smart' seems to be everywhere these days. In the context of cities, it is being applied to an increasing number of diverse projects ranging from the updating of telecommunications infrastructure to the construction of entirely new, planned cities (Halpern, LeCavalier, Calvillo, & Pietsch, 2013, p. 276). It is often used as a catchy synonym for 'intelligent', 'wise', 'autonomous', 'self-adjusting', 'resourceful', 'informational', 'resilient' and even 'ecologically friendly', thus exhibiting great semantic flexibility. However, the term has also been called a buzzword and a 'quintessential adjective of our digital age', one which promises so much yet delivers so little (Morozov & Bria, 2018, p. 2). While many practical examples of smart cities, indeed, do not deliver its promises,[16] the smart city *concept* is not as empty as it might seem. In this section, I will unpack this concept in order to find its key characteristics that will later enable me to identify the implications of such projects, particularly in connection to privacy in public space.

After at least a decade of debate, scholars are still stating that the smart city lacks a well delineated and accepted definition (e.g. Albino, Berardi, & Dangelico, 2015; Dalla Corte, van Loenen, & Cuijpers, 2017; Hollands, 2008; Kitchin, 2015b; Lombardi, Giordano, Farouh, & Yousef, 2012). While a one-size-fits-all definition of a smart city indeed does not exist, its key characteristics seem to have nevertheless been sufficiently identified in literature based on the examination of both the conceptual history of smart cities and numerous case studies of practical examples (e.g. de Wijs, Witte, & Geertman, 2016; Kitchin, 2015a; Morozov & Bria, 2018; Vanolo, 2014; Wiig, 2016). This claim is, however, limited to the conceptualisation of the smart city in the West, particularly in Europe and U.S., and does not cover different conceptualisations and practical implementations as found in Asia or Africa, which are seen as a way to enable modernisation and national development, responding to population growth, migration or managing urban transitions (Kitchin, 2015b). Nonetheless, as the focus of this Chapter and the dissertation in general is on Europe, a Western conceptualisation of the smart city will suffice.

The conceptual roots of the smart city are said to be found in the high modernist urban planning of the mid-20th century (Greenfield, 2013) and the urban cybernetics of the

16 See, for instance: Wiig (2016); Smith, K. L. (2017, November). The Inconvenient Truth about Smart Cities. Scientific American. Retrieved from https://blogs.scientificamerican.com/observations/the-inconvenient-truth-about-smart-cities/. Furthermore, *googling* 'smart city fail' will yield plenty of results with illustrative examples.

1970s (Townsend, 2013). In particular, it is based on the concepts of smart growth and new urbanism from the 1980s, which were aimed at improving the urban environment and the quality of life in cities by promoting communitarian ideas and limiting urban sprawl, land consumption and the proliferation of forms of development inspired by the logic of the automobile and personal mobility. These foundational frameworks first led to the development of concepts such as competitive cities, creative cities, sustainable cities, resilient cities and green cities (Hollands, 2008; Kitchin, 2015b; Morozov & Bria, 2018; Vanolo, 2014). By further connecting ICTs and cities, these visions came to include 'wired cities' (Dutton, Blumler, & Kraemer, 1987), the 'city of bits' (W. J. Mitchell, 1995), 'cyber cities' (Graham & Marvin, 1999), 'digital cities' (Ishida & Isbister, 2000), 'intelligent cities' (Komninos, 2002) and 'sentient cities' (Shepard, 2011). The origin of the term 'smart city', however, is not found in academic literature but in promotional literature of a technology giant – IBM, that was beginning to re-orientate itself from the traditional business model of selling hardware and software to the sale of services, including consulting (Anthopoulos, 2015; Morozov & Bria, 2018, p. 5). Based on these narratives that celebrate the march of progress and innovation, we can see that the concept of the smart city is presented as the logical high-point in the cities' technology- and information-driven evolution (Vanolo, 2014, p. 885). In this sense, the smart city is a 21st century type of utopian vision.

Based on analyses of diverse practical examples that present themselves as smart cities, at least as presented in scholarly literature, a similar but more concrete set of general characteristics can be found. These include an investment in (some sort of) digital infrastructure, a belief in the possibility of solving problems in the city through technology, and the cooperation of public and private actors in some sort of public-private partnership (e.g. Evans, Karvonen, & Raven, 2016; Morozov & Bria, 2018; Vanolo, 2014; Wiig, 2016). The public-private partnership (PPP) is a general term for describing cooperative ventures between the state and private businesses. While many different uses of the term can be found, the PPP can generally be defined as 'co-operation between public and private actors with a durable character in which actors develop mutual products and/or services and in which risk, costs, and benefits are shared' (Klijn & Teisman, 2003, p. 137). Examining these practical examples of smart cities also reveals two broad goals that this digital transformation aims for: improving urban management and the quality of life in the city (e.g. lowering gas emissions, traffic congestion and crime) and stimulating the economic development of the city. The smart city thus generally refers to the extensive embedding of software-enabled technologies, particularly ICTs, into the city environment for two broad purposes: augmenting urban management, on the one hand, and stimulating economic development of the city, on the other (Kitchin, 2015b). These two goals, of

course, are not mutually exclusive; on the contrary, they go hand in hand, as I will discuss in the following sections.

The contemporary smart city is thus made of pervasive ICTs (such as wifi, sensor and actuator networks,[17] measuring sound, temperature, movement and speed, and digitally controlled transport devices) that are used to monitor, manage and regulate city flows and process, often in real-time. These devices are also connected to and integrated with mobile computing devices (such as smartphones and laptops) used by citizens, either to engage with and navigate the city or to use them for personal communication, work and pleasure. This is done through the collection of large sets of data, mostly from public space (where the hardware is located), that are analysed in order to better depict, model and predict urban processes (Batty et al., 2012; Schaffers et al., 2011; Townsend, 2013). Such data collection is performed automatically through by networked sensor technology. Data collection and analysis are thus an essential characteristic and a priority in smart city projects, and they are often seen as providing objective, neutral measures providing robust empirical evidence for policy as well as practice (Kitchin, 2014, p. 2; Mayer-Schönberger & Cukier, 2013). These technologies – what Greenfield (2013) has termed 'everyware' – are thus said to provide a more cohesive and better understanding of the city, making it controllable in new, more fine-grained, dynamic and interconnected ways that can improve the provision of services and support sustainability.

For advocates of smart cities, another key reason for developing and implementing smart city initiatives is to help grow and sustain local economies by attracting foreign-direct investment and fostering start-ups and indigenous small and medium-sized companies in the field of digital economy (Caragliu, Del, & Nijkamp, 2009; Cardullo & Kitchin, 2018; Kourtit, Nijkamp, & Arribas, 2012). This aspect of smart cities is particularly important from the perspective of many local governments (including those in the Netherlands) facing a decline in the local economy that came with de-industrialisation, budget cuts in the public sector and the devolution of local responsibility from the

17 On the one hand, sensors are generally defined as electronic instruments that are able to measure physical quantities and generate a considerate output (usually in the form of electrical signals). Actuators, on the other hand, are devices that alter the physical quantity as they can cause a mechanical component to move after getting some input from the sensor. In other words, actuators receive control input (generally in the form of the electrical signal) and generate a change in the physical system through producing force, heat, motion, etcetera (Difference Between Sensors and Actuators. (2018). Retrieved March 31, 2019, from https://techdifferences.com/difference-between-sensors-and-actuators.html). In the *SLL* example, the video and sound cameras are sensors, whereas the smart lighting system can be seen as an actuator.

national to the local government (Van Melik, Van Aalst, & Van Weesep, 2009a). The devolution of responsibility to local governments requires resources to deal with it (e.g. more police officers or more surveillance technology to keep the streets safe). Such devolution thus comes with costs, including high financial costs, which in view of budget cuts on the state level means that cities need to find funding elsewhere. Contemporary local authorities are thus no longer solely or primarily focused on the provision of services for residents but are becoming more and more involved in the promotion of the economic prosperity of the city, its ability to attract jobs and investment, and the welcoming of investments from the private sector (Punter, 1990; Van Melik et al., 2009a). Cities have thus been re-imagined and re-classified as 'engines of development' and as actors 'responsible' for their own development (Rose, 1999; Vanolo, 2014, p. 885), which is to be achieved through entrepreneurial activity. A large part of smart city initiatives is thus a means to attract talented workers and facilitate economic activity, as well as being a new market opportunity. From the perspective of businesses that offer smart city 'solutions', however, the smart city also needs to be seen as a business model based on the provision and management of this technology that it is trying to sell in the first place. For these reasons, the smart city vision is said to be underpinned by a neoliberal ethos of market-led and technocratic solutions to city governance and development (Greenfield, 2013; Kitchin, 2015b; Morozov & Bria, 2018; Townsend, 2013).

Connected to such critiques, especially those concerning the lack of participation and the sharing of benefits by citizens, a more recent vision of the smart city putting an emphasis on the shifting of power to citizens has come to life (Cardullo & Kitchin, 2018, p. 8; Townsend, 2013). From this perspective, input from local residents serves as a counter-weight to the techno-centric, top-down approach. Smart city initiatives are thus increasingly presenting themselves as citizen-centric, claiming to generate more informed citizens, foster creativity, inclusivity, empowerment and participation. For instance, the 2016/2017 H2020 'Call for Smart and Sustainable Cities' of the European Commission expects projects to enhance citizen ownership of solutions through 'co-design, co-development and co-implementation of visionary urban planning' (see Cardullo, Kitchin, & Di Feliciantonio, 2018; see also a similar call in the Netherlands: Maas, van den Broek, & Deuten, 2017). According to the citizen-centric vision of the smart city, the strategic use of ICTs aims to foster social innovation and social justice, civic engagement and hacktivism, as well as transparent and accountable governance (Townsend, 2013). In this vision, the smart city is increasingly replaced by a newer buzzword – the 'smart society', one that provides equal opportunities and reduces inequalities (Gemeente Eindhoven, 2016; Kitchin, 2015b). It is particularly within this vision of the smart city that 'living labs' play a large and important role.

Generally, living labs are a recent type of technology development that is based on experimentation in a real-life setting with a focus on the user. However, living labs usually do not operate on their own but are deployed within or in connection to smart city projects and goals (just as is the case with the *Stratumseind Living Lab*, which I examine in Section 4). As such, they are said to promote horizontal, open and participatory smart cities that can serve all of the above identified goals: augment urban management and the quality of life in the city, increase economic competitiveness of cities and empower citizens. In the next section I will thus unpack the concept of the living lab.

3. LIVING LABS: THE CITY AS A TEST-BED

In the past decade, the city has been increasingly cast as a laboratory for the study of sustainable development (Evans et al., 2016; Schliwa & McCormick, 2016). In particular, there has been an increasing number of initiatives calling themselves a 'living lab', especially in Europe. Generally, the concept of the living lab focuses on the study of the user in her 'real-life' everyday habitat for the purposes of innovation processes (Bergvall-Kåreborn, Eriksson, Ståhlbröst, & Svensson, 2009, p. 3; Eriksson, Niitamo, & Kulkki, 2005; Kviselius & Andersson, 2009, p. 76; Schuurman, Mahr, De Marez, & Ballon, 2013, p. 6). The main promises of living labs are the design and development of future technologies that are well adapted to potential users, lowering of the threshold for social acceptance, minimisation of the risks of technology introduction, and shortening of the time-to-market (Pierson & Lievens, 2005, p. 114). It should not come as much surprise then, that initiatives and grants to establish a living lab are mushrooming today, particularly in Europe, often in connection to smart city initiatives (Maas et al., 2017, p. 7; Soetanto & van Geenhuizen, 2011).[18]

Similarly as with smart cities, the term 'living lab' has in practice become an umbrella term for a very diverse set of activities, differing greatly in focus and approach, with the only real precondition being that activities are situated in a real-world context (Schuurman et al., 2013). In view of the proliferation and growing importance of such projects that are re-creating life in the city, a more thorough analysis and

18 As stated on the website of the European Network for Living Labs, which is actually an international network of living labs, there are about 150 active Living Labs members worldwide (cca. 440 historically recognized over 12 years), excluding all other living labs that are not part of the network. See, European Network of Living Labs. (n.d.). Retrieved March 23, 2019, from https://enoll.org/.

disentanglement of the concept is needed in order to uncover its substantial relevance in practice and problematic issues (Dutilleul, Birrer, & Mensink, 2010). In the following sub-section, I will thus examine the epistemological foundations of living labs.

The concept of a 'living lab' is often credited to William Mitchell, who at the end of the 1990s used it to describe a laboratory environment with all the facilities of a regular home (Dutilleul et al., 2010; Pallot, Trousse, Senach, & Scapin, 2010; Schliwa & McCormick, 2016). This initial living lab tried to resemble a 'real' home as closely as possible and was optimised for short-term observational studies of individuals, where routine activities and interactions with technology in a 'home' environment could be observed, recorded for later analysis, and experimentally manipulated (Markopoulos & Rauterberg, 2000, p. 63; Schuurman et al., 2013, p. 3). The concept of the living lab further evolved and expanded with time and, at least in Europe, began to focus on the study of the user in her 'real-life' everyday habitat for the purposes of innovation processes (Schuurman et al., 2013). This version of the living lab thus promised a more user-centred design and development of technologies that would lower the threshold for social acceptance, minimise the risks of technology introduction, shorten the time-to-market, and introduce great social and economic benefits more broadly (Pierson & Lievens, 2005, p. 114). In order to better understand the peculiarities of this new urban development approach and offer a more convincing definition of the concept, I will follow Ballon (2015) and briefly identify the underlying epistemological background of the living lab phenomenon.

As the focus on users in real-life setting implies, the epistemological foundations of living labs can be traced to theories of mutual shaping of technology and society,[19] where technological and social change are seen as fundamentally interdependent processes (Ballon, 2015; Pierson & Lievens, 2005). An important consequence of this approach is that living lab practitioners believe that 'technologies should be studied *in situ* and in use as part of socio-technical arrangements of humans and machines joined together in action and embedded in social context' (Ratto 2000; as cited in Ballon, 2015, p. 554). Thus, von Hippel's work on innovation from the end of the 1980s is seen as an important source of inspiration for living labs because of its emphasis on the ability of users (rather than manufacturers) to create and share innovations either by developing or modifying products and services (Dell'Era & Landoni, 2014; von Hippel,

19 Thus, rejecting the perspective of technological determinism, which sees technology solely as a product and object of human activity.

1988).[20] Coupled with Silverstone's (1993) concepts of appropriation and domestication of ICTs, this resulted in the shift in focus in the innovation process from the point of purchase to the process of usage. In this sense, living labs frame the adoption of a certain new technology as an ongoing struggle between users and technology, where the user attempts to take control of the technological artefact and the technology comes to be fitted to user's daily routines (Ballon, 2015).[21] This shift acknowledges that the adoption of technology implies a modification of users' daily lives and significant, sometimes unpredictable, modifications to the meaning, features and workings of technologies (Williams & Edge, 1996).[22] The first living labs were, thus, set up as a way of structuring and operationalising new types of innovation processes through tests and experiments involving users in real-life contexts. In this sense, living labs are heavily context-based, focused on a localised environment and specific technologies, thus difficult to replicate in the same way elsewhere (Shelton & Clark, 2016).

This theoretical background led to living labs being commonly conceptualised as 'a research *methodology* for sensing, prototyping, validating and refining complex solutions in multiple and evolving real life contexts' (Eriksson, Niitamo & Kulkki, 2005, p.4, as cited in Ballon, 2015, p. 555; emphasis added) and as an '*experimentation environment* in which technology is given shape in real-life contexts and in which (end) users are considered "co-producers"' (Ballon, Pierson, & Delaere, 2005, p. 3; emphasis added). In contrast to the traditional design *for* users, living labs were intended as a participatory experiment of design *with* and design *by* users (Schuurman et al., 2013). There was thus a notable shift from passive user feedback to a more active approach based on users' involvement, leading to ideas of co-creation and participatory design.

Three chief characteristics of living labs can thus be identified from these original conceptualisations: living labs are seen as both a (1) methodology and an (2)

20 This focus was later echoed in design approaches that include user involvement such as user-centred design, participatory design and interaction design (Ballon, 2015; Ståhlbröst, 2008).

21 The relationship between the end user and the technology, which is developed apart from the end user, is perceived as an antagonistic relationship, at least to a certain extent. For instance, end users might desire certain features and functions of the product that the developers did not think of. The idea here is that by including the end-user in the development process, this 'antagonism' can be (at least partially) solved.

22 Living lab methodology is hence in line with the views of Social Shaping of Technology (SST) research, which (according to Williams and Edge (1996, p. 868) 'investigates the ways in which social, institutional, economic and cultural factors have shaped: 1. the direction as well as the rate of innovation; 2. the form of technology: the content of technological artefacts and practices; 3. the outcomes of technological change for different groups in society.'

environment for research that places the (3) citizen/user at the centre of innovation in order to better mould the opportunities offered by new ICT concepts and solutions to the specific needs and aspirations of local contexts, cultures, and creativity potentials.[23] More recently, however, the rise of online social media led to another fundamental characteristic of the contemporary living lab concept. The focus on co-creation and crowdsourcing in social media has resulted in a growing appreciation of interactions among users within communities as a source of innovation, suggesting the possibility of complex problems to be collectively addressed (Ballon, 2015). The additional cornerstone of the concept of a living lab hence emphasizes that innovation can be hindered by systemic failures such as too little interaction between innovation stakeholders (Edquist, 2001). The fourth characteristic can therefore be described as (4) open innovation, advocating for the opening up of research and development to external actors, describing living labs as 'open innovation platforms', providing a trusted environment for interactions between all relevant stakeholders, including other businesses.

Combining these four chief characteristics, resulting from the epistemological investigation of living labs, and slightly adapting Ballon's definition, we can define living labs as:

> 'an [experimentation] environment and a number of methods for organising multi-stakeholder innovation processes, including users and communities of users, in a [real-life] setting, and aimed at the exploration, co-creation and evaluation of innovations' (Ballon, 2015, p. 555).[24]

Connecting these insights to the concept of the smart city, we see that the living lab reimagines the smart city in two ways. First, the smart city or parts of it come to be seen as a beta version in need of testing through trialling, where smart infrastructures are 'white-boxed', layer by layer (Cardullo et al., 2018; Jiménez, 2014). And second, the smart city is increasingly recast as being citizen-centric – a more open, affordable, and democratic endeavour, developed bottom-up, based on needs and desires of

23 Similarly, European Network of Living Labs. (n.d.). Retrieved March 23, 2019, from https://enoll.org/.

24 In the definition, Ballon uses the term "realistic" rather than "real-life" setting, the latter of which he uses at other instances in the text and his previous writings on living labs. Because these two terms differ substantially – realistic implying that something looks real but is in fact not real, and real-life referring to an environment that is indeed real, which also follows from the epistemological origins of the concept, this paper will replace the term "realistic" with "real-life" in Ballon's definition of living labs.

local residents, where the living lab supplies the necessary skills and competences to citizens (Kitchin, Cardullo, & Feliciantonio, 2019). The deployment of living labs can thus be said to represent a bottom-up approach to the smart city, designed to increase citizens' participation and involvement in 'solving' local issues.[25] In connection to this development, the living lab approach has thus been shifted from implementations in the private sector to implementations that more closely connect them to the public sector, where it has emerged as a research infrastructure and governance tool for urban development and transitions (Schliwa & McCormick, 2016, p. 165).

While I have identified the main characteristics and definitions of (Western) living labs and smart cities in general, I will now explore how these concepts are deployed and how they operate in practice in the Netherlands, in particular within the *Stratumseind Living Lab*.

4. 'ACTUALLY EXISTING' LIVING LABS IN THE NETHERLANDS: THE STRATUMSEIND EXAMPLE

4.1 Living labs in the Netherlands: various types of collaborative initiatives

It is important to examine how smart city and living lab ideas are being grounded in particular places in the West, especially in more mature cities and economies, rather than focusing on the 'paradigmatical' smart cities of Songdo or Masdar. Particular assemblages of actors, ideologies and technologies associated with smart city/living lab interventions also bear little resemblance to the marketing rhetoric or planning and policy documents. Therefore, 'actually existing' smart cities and living labs need to be examined, rather than the idealised but unrealised visions that dominate the social imaginary and critique (adapting the notion of 'actually existing neoliberalism' of Brenner & Theodore, 2002). Living labs and smart cities are, namely, assembled in a piecemeal fashion, integrated awkwardly into existing configurations of urban governance and the built environment. This enables us to ground its critique, also in relation to privacy in public space, in particular historical and geographical context.

Before I turn to the concrete example of the *Stratumseind Living Lab* in Eindhoven, I will first briefly examine the deployment of such initiatives in the wider context of the Netherlands. In this I will follow a report of the Dutch research institute, the

25 Similarly, the European Commission, which defines living labs as *citizen-public-private partnerships* (*C3P*) or *public-private-people-partnerships* (*PPPP*); see Marana, Labaka & Sarriegi (2018).

Rathenau Instituut, which in 2017 performed a thorough examination of living labs in practice in the Netherlands (Maas et al., 2017).[26]

The Rathenau Instituut found that Dutch projects that call themselves living labs are often promoted as initiatives in which citizens, educational institutions, companies and governments (especially local governments) search together for innovative solutions for complex societal issues, such as climate change and social inequality (*ibid*., p. 7). They do this through experimental co-creation between the various actors in a real-life setting. The Rathenau Instituut (Maas et al., 2017, pp. 20–22) found that the most common actors in the self-declared living labs in the Netherlands are local governments (municipalities and provinces), private companies (large, middle-sized or small) and educational institutions (such as universities).

On paper, the focus of these self-declared living labs is on the involvement of *citizens* in the innovation process and on the development of *solutions for larger societal issues* (*ibid*., p. 15). Despite the grand claims of citizen participation, however, the percentage of participation of citizens and citizen groups (such as citizen initiatives and organisations, NGOs and housing corporations) was found to be by far the lowest of all actors, so much so, that in most of the self-proclaimed living labs no such participant was found. Finally, the Rathenau Instituut found a very diverse set of common themes of the 'living lab' initiatives, including: sustainability (with focus on renewable energy and transport), care (healthcare and care of the elderly), and city renewal and social resilience projects.

Following Schliwa and McCormick (2016, p. 174), the Rathenau Instituut defined living labs as a physical arena and a collaborative approach in which different stakeholders and actors experiment, co-create and test innovation in real-life environments, defined by their institutional and geographical boundaries. Based on two dimensions (the space of experimentation and the extent of co-creation), they distinguish between four basic types of 'collaborative initiatives' (*samenwerkingsinitiativen*): (1) open scientific research facilities; (2) industry field labs; (3) commercial urban test facilities; and (4) 'real' living labs. In view of this definition and the two main dimensions, the Instituut's conceptualisation of living labs sufficiently fits the conceptualisation I follow in this Chapter. Based on the quick-scan of approx. 90 collaborative initiatives in the Netherlands that promote themselves as living labs, the Rathenau Instituut

26 Based on a quick-scan of cca. 90 intiatives that call themselves a ‚living lab' in Amsterdam, Rotterdam, Den Haag, Utrecht, Eindhoven, Delft, Enschede, Groningen, Leiden, Maastricht, Nijmegen, Tilburg and Wageningen (Maas et al., 2017, p. 19).

found that many of them do not fulfil all or even most of the requirements of living labs.

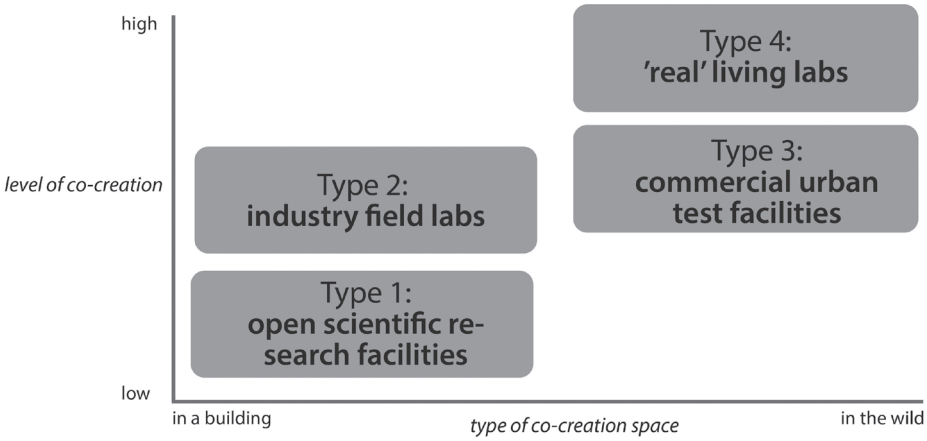


Figure 1.1: *Four basic types of collaborative initiatives (based on the figure by Rathenau Instituut, 2017)*

Open scientific research facilities experiment in a classical laboratory environment (in an enclosed environment with research facilities) and the extent of co-creation is low, as they are essentially a public-private partnership between educational institutions and private companies with a focus on research and technological development. As such, this type of initiatives should not be considered – nor should they be called – living labs. The second type of collaborative initiatives, industry field labs, typically experiment in an enclosed space or a specific test location. Essentially, the goal is to test and improve new technologies (developed by private companies) in a real-life environment. The extent of co-creation is low, as citizen and societal organisations play a very limited role in the process of innovation. While local governments do play a role in this type of project, their aim is mainly to help the (regional) industry become more innovative and competitive, indirectly making the city or region more competitive as well.

The third type, commercial urban test facilities, come closer to how the Rathenau Instituut and I have conceptualised living labs. In these initiatives, experimentation is done in a real-life setting for the purpose of developing a certain technology that is supposed to function in such an environment. As such, they also take into account non-technological aspects of innovation that they intend to test, such as marketing, use, and regulation. Nevertheless, the extent of co-creation remains rather low, as the role of citizens (and citizen groups) in the innovation process remains on a passive

level of consumer or user of new technologies, rather than co-developer. Businesses are the main players in this type of cooperative initiatives, where the goal is to innovate better and faster with the help of educational institutions, local governments and other companies. The final type are the so-called 'real' living labs, where the research is done in a real-life setting through co-creation between many different types of actors, including companies, local governments, citizens (and citizen organisations), and educational institutions. The research is focused on finding solutions to complex societal issues, where a lot of attention is given to non-technological aspects of innovation, and citizens are seen as active producers of knowledge. In this type of cooperative initiative, local governments are the leading actors, playing multiple roles: they are not only partially in charge of funding and the providing knowledge and problem input, they are also responsible for the public space (where the experiments are carried out).

The main insight from the report of the Rathenau Instituut is that 'actually existing' Dutch living labs are not just any kind of multi-stakeholder innovation project based on a type of experimental methodology. First, citizens need to be heavily involved in the development and the deployment of the technology. Second, the technology that is being developed in a particular real-life setting should aim to solve a local societal issue. This means that, ideally, where the technology is being developed (in co-creation with locals and interested citizen groups), there it should also be deployed. Moreover, since the focus of the technological innovation should be a (complex) societal issue of a particular city or part of the city, a lot of attention needs to be given to non-technological aspects of innovation, including (strongly) opposing views. This means that there should be room to discover, for example, that the imagined technological 'solution' is not suited for this particular problem in the local context. For instance, a project aiming to lower the gas emissions in a city centre by building electric car stations, should be able to discover that citizens might prefer (with good reason) to simply close down the centre (or a part of the centre) of the city to cars. Finally, the role of the municipality in living lab projects is particularly important. In order to truly promote a bottom-up, open and participatory smart city, the local government needs to hold the reigns in order to ensure that the experimentation in public space on citizens is legitimised by innovation for a widely accepted local societal purpose.

In the next sub-section, I will present a concrete example of a self-proclaimed living lab initiative in the Netherlands – the *Stratumseind Living Lab* connected to the Eindhoven smart city.

4.2 *Stratumseind 2.0* and the Eindhoven smart city

Stratumseind is a street in the centre of Eindhoven, promoting itself as the longest nightlife street in the Netherlands. It is about 400 metres long and houses around 50 establishments, such as pubs, cafés, snack bars, a nightclub and a 'coffee shop' (where marihuana is sold for consumption). It has been a popular nightlife destination, attracting a diverse and young public, for several decades. According to reports and statements from the municipality of Eindhoven, however, the number of visitors of the street has significantly decreased since around 2010 (van Gerwen, 2013). Key reasons for this are, arguably, the rising criminality and vandalism on the street. The turnover and income of the establishments on Stratumseind have decreased, some establishments have closed, leaving empty slots on the street, further making it a less attractive destination. Consequently, the Stratumseind street got a bad image. According to Eindhoven municipality, these are the key reasons for the *Stratumseind 2.0* project, which had begun in June 2013 and lasted until 2017 (*ibid*.).

Figure 1.2: *A 3D map of the Stratumseind street (copyright Nikkie den Dekker)*

Stratumseind 2.0 is a project in the form of a public-private partnership between the municipality of Eindhoven, the police and a range of private parties, including the Stratumseind establishments association, real-property owners on the Stratumseind street, and Dutch breweries (Grolsch, Heineken, Bavaria and the InBev conglomerate). It is essentially an umbrella project, entailing an increasing number of sub-projects. In view of the reasons for the project, the main objective of *Stratumseind 2.0* is to 'long-lastingly improve the street from an economic as well as a social point of view' (*ibid*., p. 2; translation by author). In other words, the main idea is to keep Stratumseind nice

and safe but also – or moreover – to provide a good business model for all of the actors involved. The project thus has three main themes: safety, 'livability' (*leefbaarheid*) and attractiveness. More concrete goals of the project are:

(1) to attract more visitors, make them stay longer and spend more money in the establishments;
(2) lower the vandalism, police and health-related costs in connection to Stratumseind;
(3) lower the energy, security and waste costs in connection to Stratumseind;
(4) increase the real-estate value and the income related to the Stratumseind street and the city of Eindhoven as a whole; and
(5) create positive value of direct marketing (Eindhoven, 2015).

These ambitious goals are planned to be achieved through a variety of means and initiatives, especially through 'a 365 days, 24/7 scan of all data on Stratumseind' in order to gain valuable insights from the analysis performed on 'Stratumseind data' (Kanters, 2013; Kanters & van Hoof, 2014). The key element and the main sub-project of Stratumseind 2.0 is thus its living lab – the *Stratumseind Living Lab* (*SLL*).[27]

This project is connected to a broader transformation of Eindhoven into a smart city. This transformation is not particularly surprising, as Eindhoven is a city with a well-known technical university, where several technology companies are already present, including the multinational company Philips. Furthermore, in 2011 the region of Eindhoven and surrounding cities, termed the 'Brainport region', has been proclaimed the 'smartest region in the world' under the theme Health & ICT by the Intelligent Community Forum (ICF).[28] In 2014, within the Triangulum project,[29] a consortium consisting of Eindhoven municipality, private businesses and the Technical University Eindhoven was granted a subsidy of €6,4 million by the European Commission in order to further transform Eindhoven into a smart city, alongside other similar projects.[30] In

27 Besides the SLL, which will be the main focus of this Chapter, Stratumseind 2.0 includes a few non-technology related initiatives, including the ‚Glass project' (in which glass cups are not allowed on the street, being replaced by plastic cups) and the 'Terrase plan' of the Eindhoven Police department's Horeca team (a police team that patrols the streets in the centre of Eindhoven during going out nights); see van Gerwen (2013).

28 See European Commission. (2011). Brainport region is the "smartest region of the world." Retrieved March 19, 2019, from https://ec.europa.eu/digital-single-market/en/news/brainport-region-smartest-region-world.

29 See Triangulum project. (n.d.). Retrieved March 23, 2019, from https://www.triangulum-project.eu/?page_id=2137.

30 See Mol, Khan, Aalders & Schouten (2015).

particular, the projects concern the creation of sustainable living environments, such as renovations creating energy-efficient housing, the introduction of electric buses, and innovative lighting installations in public space. The main goals of the project are: (1) strong participation of the citizens; (2) smarter functioning of the administration; (3) a development of the open data network in the city; and (4) co-creation as a guiding principle (Mol, Khan, Aalders, & Schouten, 2015). Within this initiative, technology is clearly seen as a means to improve the quality of life in the city.

Furthermore, reviewing policy documents of Eindhoven municipality, we see that the 'smart city' term has been replaced by the newer 'smart society' term (Gemeente Eindhoven, 2016). According to the policy document, while a smart city is all about efficiency (how to improve urban management with a more efficient use of ICTs and data analysis), the smart society focuses on improving the quality of life in the city, which is to be achieved through cooperation and co-creation with citizens (*ibid*., p. 3). The main idea of this transformation is that the city opens itself up as an 'experimental environment' (*proeftuin*) for businesses and educational institutions for the purpose of improving well-being, attracting jobs and sustainability (*ibid*., p. 3). The goal thus is to create a vibrant city with active and healthy citizens, a good economic climate and strong social networks, as well as a sustainable city with social wealth, caring for the environment and a sustainable economy (Kanters, 2016). Such a smart city (or society) is to be achieved through various means, among which living lab initiatives play a vital role – through experimentation in real-life settings and a horizontal (rather than vertical) approach they enable the co-creation of the best technological solutions (Gemeente Eindhoven, 2016, pp. 25–30). Indeed, there are already several (self-proclaimed) living labs in Eindhoven: besides the *Stratumseind Living Lab*, also the *Strijp-S* and *Eckart Vaartbroek*. Eindhoven thus promotes itself as a 'city as a living lab' in which potential new solutions are explored (*ibid*., p. 25). What exactly this means in practical terms, I will examine in the next sub-sections, where I describe in detail the deployment and operation of the *Stratumseind Living Lab* and its sub-projects.

4.3 The *Stratumseind Living Lab*

The *Stratumseind Living Lab* (*SLL* or *Living Lab*) is described as a field lab with a variety of sensors, mostly positioned on the Stratumseind street itself, and various actors, with the intention of measuring, analysing and stimulating the behaviour of people in public places (Kanters & van Hoof, 2014). It describes itself as a combination of 'smart sensors, smart interfaces, smart actors, smart lights, smart data and smart design' (Kanters, 2016). Like *Stratumseind 2.0*, the *SLL* is also an umbrella project organised in the form of a public-private partnership. As an umbrella project, the *SLL* is mainly a common name to a growing number of sub-projects with diverse goals (ranging from

crime prediction and community policing to de-escalating people's behaviour via light and smell, and community building) and actors. From its beginning up until 2018, the *SLL* included the following projects: *CityPulse*, *De-escalate*, *Trillion*, *Stratumsepoort*, and *Scorpion*. The *SLL* officially lasted from mid-2014 to mid-2018, however, some of the projects seem to be continuing with several of the same parties still in 2019.[31] I will examine three of the *SLL* sub-projects concerning crime prediction, de-escalation of persons' behaviour and community policing – that is, *CityPulse*, *De-escalate* and *Trillion,* in the following sections of this Chapter. I have chosen these sub-projects as they were the largest and most long-lasting projects with potentially the highest impact on privacy in public space.

The *SLL* public-private partnership involves a large and growing number of actors. Public parties, on the one hand, include Eindhoven municipality, the police and local higher education institutions, including the Technical University Eindhoven and Tilburg University. On the other hand, private parties mainly include various technology companies, global and large (multinationals such as Philips, Atos and Cisco) as well as local and smaller businesses (like Sorama and Vinotion). The municipality is the common denominator to all of the projects, occupying a central role in the *Living Lab*. Nevertheless, the information and communication technology (ICT) companies play a role that is at least or even more important. Without their willingness to provide their technologies (hardware and software) and services for a symbolic fee (as follows from my interviews with the *SLL* parties), the *Living Lab* and its growing number of sub-projects would not be possible (although a smaller amount of funding comes from public sources, such as Eindhoven municipality and the North Brabant province; see van Gerwen, 2013).

Technology companies are willing to provide their technology and expertise for free expecting a large and lasting economic growth. As a representative of Atos, one of the key parties to the *Living Lab's CityPulse* project put it, the idea is to sell the *CityPulse* system for detecting and predicting crime and disturbances in urban areas across the world (Kist & van Noort, 2015). Stratumseind is therefore seen as a free test-bed for the testing of new technologies in real streets, real situations and on real people, in an attempt to eliminate the bugs and brittleness of technological systems that are being developed. In the race of keeping cities competitive, the municipality of Eindhoven welcomes such projects with open arms. As the Alderman of Eindhoven municipality at the time, Bianca Kaathoven, put it: 'We are also looking for tangible results. But our

31 See Stratumseind Living Lab. (2019). Living Lab, Stratumseind 2.0. Retrieved March 19, 2019, from https://www.facebook.com/LivingLabStratumseind/.

main concern is that we open up Eindhoven as a laboratory for innovative companies' (as cited in Kist & van Noort, 2015; translation by author). While the municipality has the role of coordinator and facilitator of the projects (ideally, providing the proper legal backing and setting the limits for experimenting in the wild), because of their practical dependency on private companies, the latter can to a great extent dictate the terms on which they will provide their technologies. From this perspective, the *SLL* is greatly dependent on businesses – their technology and funding – meaning that these private actors should be seen as the key, most powerful actors of the project.

Furthermore, the *SLL* also includes higher education institutions among its parties, for instance the Technical University of Eindhoven (TU/e) and Tilburg University (TiU).[32] These either take part in the development of the technology itself (as in the case of TU/e in the *De-escalate* project) or they can perform legal and theoretical assessments of the activities within the *Living Lab* (as is the case with the present author).

The main goal of the *SLL* as a whole, as described by Eindhoven municipality, is to gain insight into the question, 'in what ways can external stimuli (substantially) influence the *escalating* as well as *de-escalating* behaviour of visitors of the street' (Kanters & van Hoof, 2014). This question also forms the primary research question of the project. This document also lists six additional research sub-questions:

(1) What are the problems recognised on the Stratumseind street?
(2) Which external stimuli have an effect on the behaviour of people?
(3) Which stimuli can be applied to the Stratumseind situation?
(4) Which stimuli can be measured and how?
(5) Are there any connections between the different stimuli?
(6) How do the stimuli behave in regard to either influence or stimulation? (*ibid.*; translation by author).

32 The author's PhD is a part of this research, examining the legal implications, with a focus on the right to privacy, of the *SLL*.

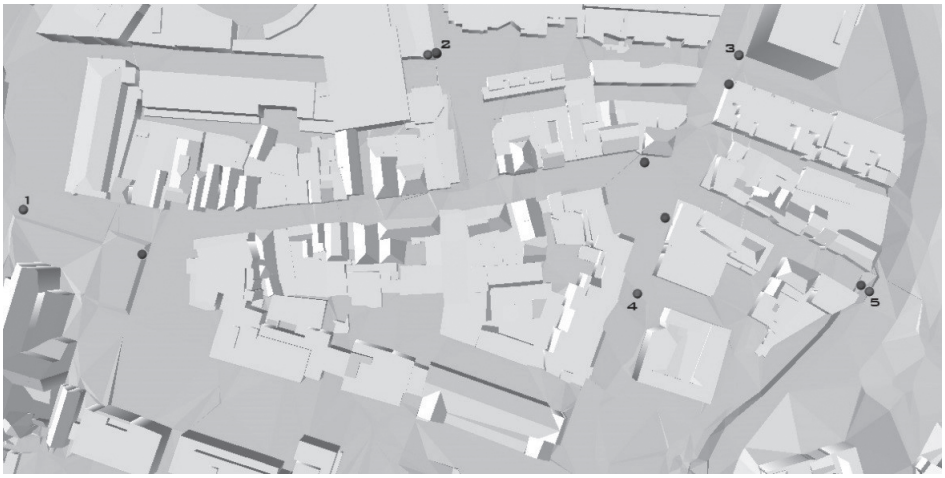


Figure 1.3: *Locations of video cameras and sound sensors on the Stratumseind street (red dots are video cameras, blue are sound sensors) (copyright Eindhoven municipality)*

In order to achieve these goals, the *SLL* employs a large number of increasingly sophisticated digital technologies that generate, store and analyse diverse types of data somehow connected to Stratumseind ('Stratumseind data'). The functioning of the *SLL* is thus based on data capture, processing and storage, as well as on the integration of the various sensor technologies. The *SLL* includes various sensors and actuators that are mostly positioned on the Stratumseind street, including: video cameras (with embedded analytical capabilities; five cameras on or near the Stratumseind street), sound sensors (six sensors on and near the street) and sound cameras[33] (embedded with additional analytical capabilities), special lighting and olfactory technology (that emits smells), *CityBeacons* (large objects combining the functions of cameras, information signs, signposts, antennas, advertising spaces and video screens), wifi tracking, technology for social media sentiment analysis, and a weather station (measuring temperature, wind strength, precipitation and sunlight).

All of the data that is continuously captured or generated via these sensors, as well as other data collected through non-technological means (such as statistical data from the police, breweries, garbage services and parking garages), are being stored in a database in order to create a 'knowledge discovery database' that can be utilised through data analysis techniques. Data that is captured and collected include: the number of people approaching and moving away from Stratumseind, people density on the street, persons' walking patterns, the total number of people, stress levels in people's voices,

33 The precise number of these is unknown to the author.

the nationality and hometown of the visitors (based on smartphone subscription data received from Vodaphone), the average sound level on the street, petty, moderate and serious crime levels on the street (based on police statistics), the number of tweets with 'Stratumseind data', the percentage change of beer ordered by the Stratumseind establishments (weekly), volume of garbage collected from Stratumseind (weekly), tons of glass from the street collected (weekly), the number of cars parked in certain car parks in the centre of Eindhoven, the temperature, wind speed and direction, and the amount of rainfall per hour. The *SLL* also entails a 'basecamp' – a physical location on the Stratumseind street, where big screens visualise the real-time collection and analysis of all of these data. Yet, throughout the lifespan of the *SLL* sub-projects, there was no sign on the street that would notify citizens of the various activities happening there.

4.3.1 *CityPulse:* a predictive policing project

The *CityPulse* project, a project developing a system for detection of deviant behaviour and atmosphere on the street, was one of the biggest projects that took place within the *SLL* from 2015 to end of 2017. Some of the world's biggest ICT companies, such as Atos (funded by IBM for this project) and Intel, were parties to this project. Other actors included the Eindhoven municipality, the police, DITSS (Dutch Institute for Safety and Securty; a non-profit organisation), and a few smaller, local technology companies, such as Vinotion and Sorama. Employing a variety of sensors on the Stratumseind street and social media analysis, the *CityPulse* system was intended to create 'a powerful picture of the street and help authorities better predict and react to situations and de-escalate them before they develop' (Atos, 2015). In this sense, the *CityPulse* project was a type of predictive policing projects that have increasingly been taking place in the last decade worldwide, including in the Netherlands (Schuilenburg, 2016).

In particular, this project employed video cameras, sound sensors and sound cameras with embedded analytical capabilities, as well as data created by other sensors, such as the temperature, wind speed and rainfall (mentioned above), and data gathered from weekly statistics. The *CityPulse* system thus supposedly knows how many people are walking or biking around on Stratumseind at any time of the day, which bar is the most crowded, how fast persons are moving and who has a suspicious walking pattern (Kist & van Noort, 2015). The system also performs sentiment analysis of *tweets* that relate to the Stratumseind street – for example, a tweet that is posted from the physical location on the street or mentions chosen 'Stratumseind keywords', such as the street name, a bar on the street or a famous bartender there.

The *CityPulse* system was designed to analyse all of these types of data, looking for anomalies in data patterns, which could then be cross-referenced against other gathered data sources. If these data sources would confirm the likelihood of an incident, the system would alert the regional police control room (*regionale toezicht ruimte*), giving the police an opportunity to make better informed decisions on any action on the Stratumseind street that might be required (Atos, 2015). This would be done through an application (app), first requiring human authorisation but acting autonomously when fully developed, which would be a direct link between the *SLL* and the police. The app would have four possible notifications or 'buttons': 'nothing wrong', 'everything alright', 'backup needed' and 'high risk situation'. The *CityPulse* system, could also adapt the lighting colour and levels on the street (a technology developed in another *SLL* sub-project, *De-escalate*, which I discuss in the next Section). The system was thus seen as a predictive, preventative and an ancillary tool for the police in its role for crime and order maintenance in the city. Although it was planned that the system would eventually be able to act on its own, for example, predicting or at least detecting a fight in real time and notifying the police about it, this capability was not realised; a human agent remained required to authorise the notification to the police.

There were high expectations of this project. The *CityPulse* system was expected to make the Stratumseind street a safer and friendlier nightlife environment. Law enforcement was expected to be deployed in a more efficient manner, resulting in fewer incidents. Additionally, the costs of clean-up and repair work for both the city and the establishments on the street were expected to be reduced. The parties of the project have also stated that this way of producing insight can be extended to a variety of other areas, including giving citizens alerts when air pollution levels reach a certain threshold, automatically redirecting traffic, when parking or congestion parameters are reached (Atos, 2015). This fits well within the smart city vision and implies the possibility of a range of new sub-projects within the *SLL*.

Since this project has already ended, a brief analysis of its results (at least those that were shared with the author in the interviews) can be made. First, the results of the Twitter sentiment analysis were not particularly successful. The type of sentiment analysis that was performed was very simple, sorting tweets with 'Stratumseind keywords' into positive, negative and neutral. However, the number of tweets with these keywords remained very low, implying that people do not tweet about Stratumseind too often. Furthermore, the vast majority of tweets was perceived by the system as neutral, thus, which was seen as useless for the goal of the system – detection of a positive or negative 'atmosphere' on the street. It was thus impossible

to draw statistically significant conclusions from the data. Second, the *CityPulse* system was able to detect a fight happening on the street but no predictive or preventive capabilities were achieved. According to the parties of the project, this was partially due to the insufficient number of fights on the street in the time of the development of the system (sometime between 2015 and 2017). Since a police officer on the street itself or one behind the police CCTV is also capable of detecting a fight happening on Stratumseind (and to then deploy a nearby officer to the spot), these are disappointing results. Moreover, as there were not enough fights on the street to develop any further analytical capabilities of the system, it is reasonable to question the need for such extensive surveillance on the street in the first place. Finally, no data has been shared with the author or the public on the reduced costs related to Stratumseind or its perception as a nicer and safer nightlife environment. Based on these results, it would be difficult to claim that the *CityPulse* system has contributed to the making of the Stratumseind street any safer, more pleasant or less costly.

4.3.2 *De-escalate:* influencing people's behaviour with the use of light

The *De-escalate* project was a project developing a special lighting system with the purpose of influencing and diffusing 'escalated' mood and behaviour with 'dynamic lighting scenarios' in public space, such as on the Stratumseind street, or in small-scale indoor settings, such as prisons, psychiatric wards and help desks. This project run from 2014 to 2018 and was led by researchers from the Technical University of Eindhoven (TU/e) and Philips, a large Dutch technology company from Eindhoven, which designed and provided the lighting system. Other, smaller, parties to the project include Eindhoven municipality, the police, DITTS and other smaller technology companies.

The *De-escalate* project is described as an intelligent lighting system to control emotion (de Kort, 2014, p. 10). The project experimented with the effect of interactive lighting design in 'de-escalation' of aggressive behaviour, based on psychological pathways through which exposure to dynamic lighting could defuse escalating behaviour. Within this project the Stratumseind environment was explored and Stratumseind visitors were profiled in order to find out what causes aggression and escalation on Stratumseind and how such behaviour can be measured and, furthermore, to explore the possibilities for dynamic light designs, which could reduce these escalation/aggression levels (Kalinauskaitė, 2014, p. 4). In this sense, it can be seen as a nudging tool or, more broadly, a tool that influences people's behaviour and, potentially, impairs persons' autonomy (I discuss this issue in Chapter 5).

There are two key terms used throughout the project: escalation and atmosphere. The first term, 'escalated behaviour', is used in a very broad sense within this sub-project and the *SLL* in general, referring to all types of behaviour of persons who in some way lose self-control, including screaming, getting abusive, aggressive or crossing other behavioural boundaries that a person would otherwise not cross (de Kort, 2014, p. 10). Escalation, then, refers to 'an increase in severity of aggressive means used in a given conflict' (Winstok, Eisikovits and Fishman, 2004, 284; as cited in de Kort, Ijsselsteijn, Haans, Lakens, Kalinauskaitė, et al., 2014, p. 94). The extent of escalation thus ranges along a wide dimension of intensity, from frustration and annoyance to rage and being out of control. Escalation typically involves a narrowing of attention and progressive failure of cognitive and executive functioning, potentially resulting in risk taking and 'commitment to aggression' (de Kort, Ijsselsteijn, Haans, Lakens, & Kalinauskaitė, 2014, p. 94). On the physiological level, escalation involves increased blood pressure, total peripheral resistance, and facial warming (*ibid.*). Escalating persons therefore fail to control their emotion and emotion-driven urges as a function of both internal state (stress, arousal) and/or external cues (time, place, audience).

The second key term is atmosphere. Since aggression (connected to the broader concept of escalated behaviour) is behaviour that is strongly dependent on context (including crowding, noise and temperature), socio-physical characteristics of environments can coerce behaviour in dynamic but patterned, and thus predictable ways (Kalinauskaitė, Haans, de Kort, & Ijsselsteijn, 2018). Most often, aggression and escalation occur not because they were intentionally planned, but because people respond to perceived stress, become ignited by autonomic arousal and anger and in this process break personally held norms and revert to things they might not do otherwise. *De-escalate* researchers thus wanted to affect the 'atmosphere' on the Stratumseind street in order to de-escalate aggression. They defined 'atmosphere' as 'people's attitudes, mood, behaviours and interactions with one another as well as with their immediate environment' (Kalinauskaitė et al., 2018). It is thus seen as a characteristic of social context that can be transformed into measurable data, coloured through interactions with other visitors. Atmosphere, however, is dynamic – it changes continuously and is therefore difficult to affect and control. This abstract term was seen as being of value, as the police and the security staff on the Stratumseind street often refer to it and use it in order to evaluate the general situation on the street and anticipate people's behaviour. In other words, atmosphere was seen as an important indicator of the risk of incidents and escalations (*ibid.*, p. 229).

The *De-escalate* project thus aimed to provide insights into human behaviour and deliver lighting schemes applicable and effective in real-time conditions in order to

de-escalate behaviour on the street. In other terms, the goal is to produce more 'social' and less aggressive behaviour (de Kort, 2015, p. 20). This was planned to be achieved particularly through the use of light in relation to attention and (self-)awareness (*ibid*., p. 18). Literature shows, for instance, that dim and warmer colour light is associated with lower arousal, with studies showing that exposing people to pulsating orange light at slow frequencies leads to relaxing breathing rhythms (Smolders, de Kort, & Cluitmans, 2012). Directed or bright light can, according to de Kort (2015, p. 18), heighten self-awareness, whereas darkness can trigger feelings of anonymity. If in darkness we can go undetected, in spotlight persons are vulnerable to the scrutiny of others. The awareness of this loss of anonymity may turn a person's attention to their inner states and traits, and prompt them to examine their personal norms and engage in better self-regulation (de Kort, 2015; referring to Steidle & Werth 2014; Carver & Scheier 1979; Duval & Wicklund 1972). De Kort is thus echoing the ideas of Bentham and Foucault on the Panopticon and discipline – that is, that the awareness of being watched makes the person abide by the external norms, while also internalising them (I discuss the following in Chapter 2 on surveillance). Nudging with light might thus be seen here as an indirect manner of disciplining people.

The project made use of analysis of the data of incidents in the past, open data and social media data, trying to find correlations with all kinds of potentially influencing factors (such as weather, results of a football match) (den Ouden & Valkenburg, 2013, p. 156). With the use of such data analysis predictions were made on the stress levels that put the lighting system in motion, aiming to proactively keep stress levels at 'acceptable levels' (*ibid*.). What these 'acceptable levels' are, however, was not defined. As is clear from this description, the *De-escalate* project is heavily based on insights from psychology, especially environmental psychology, turning the 'technological solution' of an issue far less neutral and objective as it might seem from the living lab/smart city rhetoric of providing 'technological solutions to social issues' (this is one of the issues that I discuss in Section 5).

The project has an additional aim – the development of a new market for dynamic lighting scenes and interactive applications (den Ouden & Valkenburg, 2013, p. 157). This can be connected to the possibility to escalate behaviour, when the atmosphere on the street is too sleepy or boring, which has also been mentioned in the policy documents of Eindhoven municipality (Kanters & van Hoof, 2014). Since one of the main goals of the *Stratumseind 2.0* is to attract more visitors to the street, make them stay longer and spend more money in the pubs there, thus also getting more intoxicated, it is not too far-fetched to imagine that the lighting system would also be

used to 'escalate' the atmosphere on the street, making people more active and more thirsty (I explore this idea further in Chapter 5).

Performing research in an uncontrolled or real-life environment, such as the Stratumseind street, is of course incredibly challenging. TU/e researchers participating in *De-escalate* were aware from the beginning that isolating individual dimensions of context in order to study the effects of light, especially in public space, may prove to be very limited or even impossible (de Kort, 2015, p. 22). While the project has ended, concrete results are not available to the author or the general public. In fact, the project's website, where information and academic output connected to the project were gathered, has already been taken down.[34] What can be gathered from the information available, is that the project did not end in any particular success. Kanters, the *SLL* project leader from Eindhoven municipality, has stated in an interview that the *De-escalate* project has not resulted in any tangible de-escalating effects on aggressive behaviour on the Stratumseind street:

> 'We thought that that the atmosphere could be influenced in this way [with dynamic lighting scenarios] but this was not the case in practice. In any case, it is hardly measurable. The number of incidents is decreasing but there are also fewer visitors' (Hoekstra, 2017; translation by author).

What will happen with the lighting technology on the street and the gathered data is unclear. While this type of nudging people's behaviour seems rather benign, it can also lead to a slippery slope in regard to the municipality and businesses that take these pilot projects (regardless of their failing or succeeding) as a general stamp of approval of nudging people's behaviour with various sources. Indeed, the municipality is already continuing the testing of nudging people's behaviour, this time with the smell of oranges.[35]

4.3.3 *Trillion:* community policing

The *Trillion* project is a project concerning community policing, developing a community policing platform in the form of an application (app), which aims to facilitate effective cooperation between citizens and law enforcement agencies (LEAs). The idea is that citizens will be able to support the achievement of – what the stakeholders call – a better 'urban security management' through reporting crimes,

34 See: http://www.de-escalate.nl/; the website does not work anymore (accessed 07 November 2018).

35 See: van de Nieuwenhof, J. (2015). Een kijkje in het Lab van het Stratumseind. Retrieved March 23, 2019, from https://innovationorigins.com/nl/een-kijkje-in-het-lab-van-het-stratumseind/.

suspicious behaviour and incidents, identifying hazards and assisting LEAs through active participation. While the idea of community policing with the use of social media is not new,[36] the *Trillion* App promises to have additional functionalities, which I present in the following paragraphs. LEAs will, thus, supposedly detect incidents in a more efficient, content- and context-aware manner, locate on-site citizens, other LEA representatives and first responders, communicate with them, request more information, and assign specific actions to address ongoing incidents. In other words, the project 'aims to deliver a comprehensive multiple channels platform for incident discovery, prediction, reporting and interaction' (Sorace, 2016). As such, it aims to contribute to a safer society, improving both objective safety (e.g. crime statistics) and subjective safety (e.g. fear of crime and trust in the police). It is a European Union (EU) H2020 project that received a research and innovation grant, with partners from the industry (technology companies, including Atos), municipalities and law enforcement departments (including from the Netherlands, Italy and the UK), as well as a few educational institutions. While the project claims to be user- or citizen-centric, no citizen groups are found among the stakeholders.

Through the app, either on a smartphone, computer or wearable devices (e.g. smart watch), citizens will be able to report crimes as well as anti-social or suspicious behaviour and other incidents, identify hazards and actively assist law enforcement agents (Patrikakis et al., 2018). In order to develop the app so as to suit both law enforcement and citizens' needs, the app was tested in several real-life settings (including on Stratumseind in Eindhoven) via certain scenarios. A gaming approach was thus adopted in order to train users on how to use the app. This means that citizens can play a variety of 'serious games'[37] with several scenarios to choose from, which – at the end of the game – encourage citizens to download the *Trillion* app and use it in real-life situations. Law enforcement agencies also played the game (Sorace et al., 2018). The chosen scenarios touched upon four themes: 'crime and justice' (examples of crime reporting, including trafficking, domestic violence and drug dealing in a pub), 'event and crowd management' (example of a crime and antisocial behaviour at a concert), 'public protection and disaster relief' (example of a natural

36 Similar initiatives, including Burgernet (www.burgernet.nl) and Meld misdaad anoniem (https://www.meldmisdaadanoniem.nl/) have existed in the Netherlands already for a while. These initiatives also use social media and Apps to engage citizens in addressing crimes and incidents (e.g. the Burgernetapp).

37 A serious game (also called an applied game) is a game designed for a primary purpose other than pure entertainment, such as for purposes of defence, education, scientific exploration and city planning (Djaouti, Alvarez, & Jessel, 2011).

disaster, such as an earthquake) and 'emergency and public safety' (with sub-themes of fires in a rural or urban environment and cybersecurity) (Sorace, 2016).

A user can create and send a report in three steps. According to Patrikakis (2018), in the first step the user chooses a type of incident from a predetermined list, which includes: 'vandalism and behaviour', 'bullying', 'suspicious behaviour', 'racism and hate crimes', 'graffiti and destruction, 'antisocial behaviour' and 'other'. Whilst trying out the app as tested in Eindhoven myself, I noted somewhat different possible incidents to report. It included possibilities such as, 'abuse of alcohol' (*alcohol misbruik*), 'threat' (*bedreiging*), 'fight' (*gevecht*), 'burglary & robbery' (*inbraak & overval*), 'spyware' and 'traffic accident' (*verkeersongeval*) (see Figures 4 and 5). In the second step, a brief description of the incident is required. In this step the user can also attach media files, including image, audio and video (either existing or directly recorded via the app; this is an additional feature that the mentioned community policing initiatives in the Netherlands do not have). In the final step, she can review and modify the report, and include her identity or not. When one user sends out a report, all other users in the vicinity with the app installed on their device receive an alert of the event.

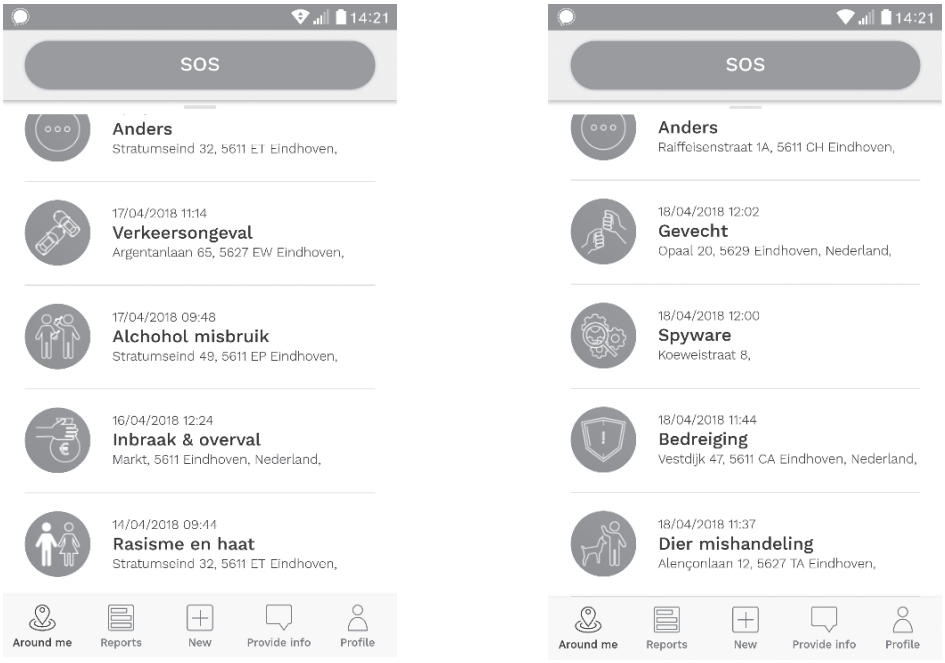
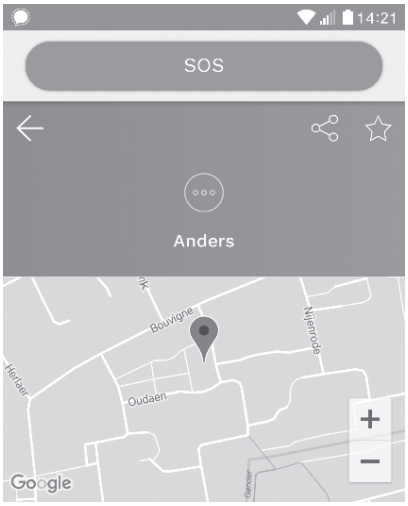
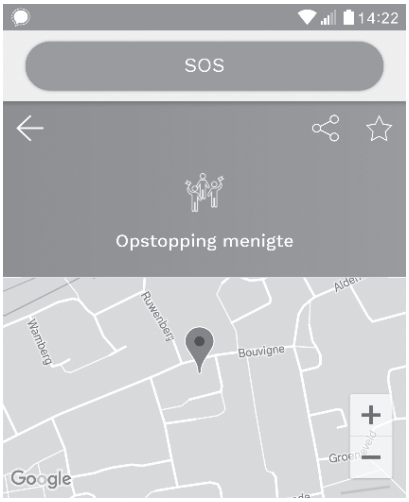


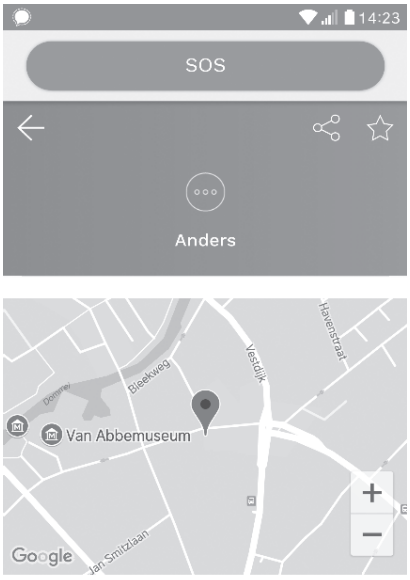
Figure 1.4: *Author's screenshots of the Dutch version of the* Trillion *App (taken on 2 May 2018)*



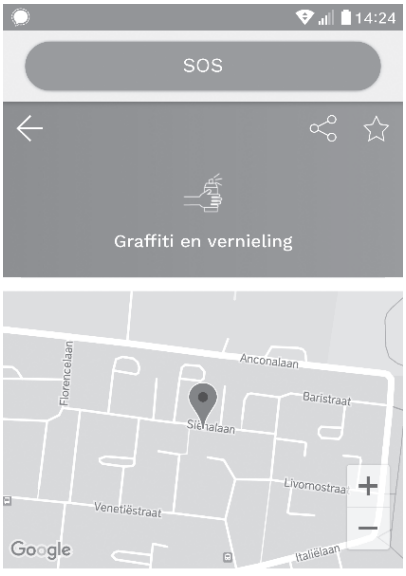
REPORT DESCRIPTION
Mensen die luidruchtig praten en lachen, vermoedelijk teveel gedronken en door de wijk heen lopen.



REPORT DESCRIPTION
Op de Bouvigne is een demonstratie aan de gang tegenstanders van de koning. Dit loopt een beetje uit de hand want de demonstranten worden tegen gehouden door voorstanders van de koning



REPORT DESCRIPTION
Overlast van de muziek



REPORT DESCRIPTION
Graffiti bij winkelcentrum vaartbroek

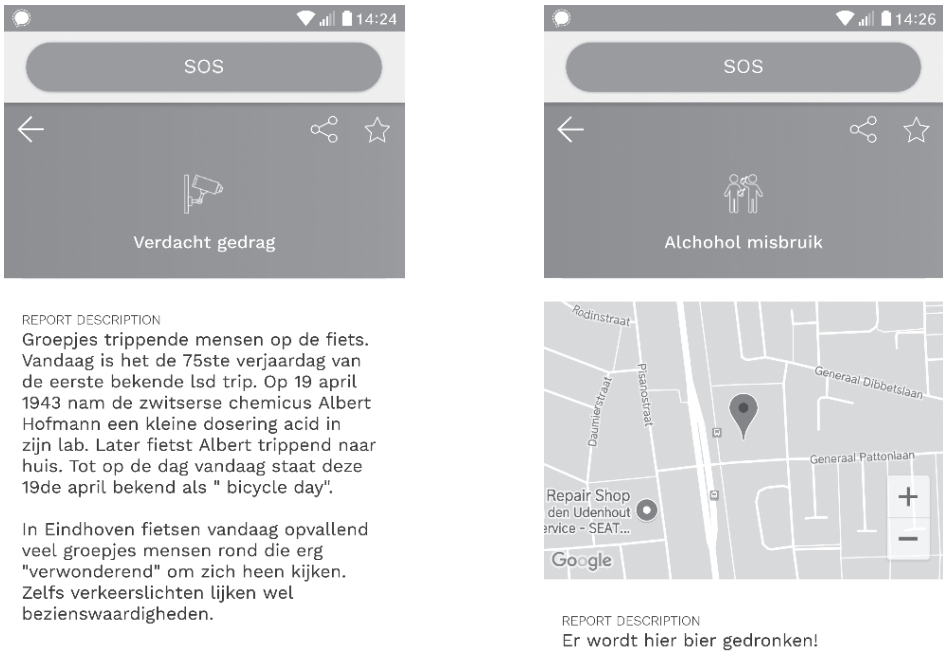


Figure 1.5: *Author's screenshots of the Dutch version of the* Trillion *App (taken on 2 May 2018)*

The above screenshots in Figure 1.5, which I took during the testing phase of the project in Eindhoven (between 16 April and 28 May 2018), represent 'test-reports', that is, reports that are not based on actual incidents, from 300 participants asked to report possible incidents through the app (van Arensbergen, 2018). As such, they can offer insight into how residents of Eindhoven (at least those that were willing to participate in the project) see the app could and should be used. For instance, we can see that a report was made 'beer is being drunk here!' (*Er wordt hier bier gedronken!*), there are 'graffiti at the Vaartbroek shopping centre' (*Graffiti bij de winkelcentrum vaartbroek*), there is 'nuisance because of loud music' (*Overlast van de muziek*) and there are 'people talking loudly, probably because they drank too much, and will likely walk through the neighbourhood' (*Mensen die luidruchtig praten en lachen, vermoedelijk teveel gedronken en door de wijk heen lopen*). The last two reports concern a demonstration against the King, which 'got a bit out of hand due to opposition from the supporters of the King' (*Dit loopt een beetje uit de hand want demonstranten worden tegen gehouden door voorstanders van de koning*) and a celebration of the discovery of LSD, where remarkably many groups of persons were biking while obviously high on the drug – 'even traffic lights seem like sights' to them (*In Eindhoven fietsen vandaag opvallend veel groepjes mensen rond die erg 'verwonderend' om zich heen kijken. Zelfs verkeerslichten lijken wel bezienswaardigheden*).

While some of these reports have clear value in connection to public safety, such as the example of the celebration of the discovery of LSD by biking high through the city, others seem to have it less. This can especially be seen in the reports on beer being drunk in public space and on the group talking loudly and walking around the neighbourhood. While consuming alcohol may result in drunkenness and the group might indeed be looking for trouble, it might also be an example of *gezelligheid* or conviviality that people from the Noord-Brabant province pride themselves on. Unless we want to tightly script what is proper and acceptable behaviour in public space, such activities *in themselves* should not be granted the attention of law enforcement. Concerning the demonstration, it is difficult to see the added value of such a report via the *Trillion* app. Demonstrations in the Netherlands namely require either a prior notification of the municipality or, in the case of large-scale and risky events, a permit.[38] As a consequence of this notification, authorities decide whether the presence of law enforcement might be needed, which in the case of a demonstration against the King, would likely be deemed so. The police would thus already be present on site, making sure that the confrontation does not get too much out of hand.

One of the main identified challenges of the project was the facilitation of trust between citizens and LEAs, which is needed for community policing. While the project introduced several technologies for community policing, it was clear to the parties that its success will finally depend on societal approval and the actual adoption of the technology. That is why a large part of the project was said to be concerned with achieving high societal approval. While this sounds promising, it was aimed to be achieved mainly (or solely) through technological means, namely data protection- and privacy-by-design. This means that the app would be designed in such a way so as to facilitate the protection of personal data, while ensuring the usability of the deployed tools, so that they are easy to master and use. The app was thus designed to have a simple user interface, including an easy to understand data security system (for instance, by displaying a score of 'cyber trustworthiness' of the device to the user) (Patrikakis et al., 2018). How this 'cyber trustworthiness' would be measured, by whom and how to convince the users that the assessment should be trusted, however, was not explained. Relating to the protection of privacy, the app also has certain privacy by design features, such as the possibility for anonymous uploading of a report and the blurring of faces in the visual content uploaded (*ibid*.). Nevertheless, the app has

38 See, e.g.: Gemeente Rotterdam. (2019). Vergunning B- en C-evenement. Retrieved March 31, 2019, from https://www.rotterdam.nl/loket/vergunning-b-en-c-evenement/; based on Art. 2.25 of the Rotterdam Municipal ordinance (*Algemene Plaatselijke Verordening Rotterdam*) in line with the Public Events Act (*Wet openbare manifestaties*).

an obligatory registration (requiring one's name, surname and contact information, such as an email) in order to deter false reporting. While fake information can, of course, be provided for registration purposes, this does not seem like a good option in this project, where trust is essential. Furthermore, depending on the actual software, an anonymous uploading of a report might still be traced back to an individual user of the system.

The issue of trust between law enforcement and citizens is a complex matter, highly dependent on context (see e.g. Noor & Metwally, 2018). As such, it goes much beyond the topic of this Chapter. Nevertheless, I want to briefly point out that in the particular context of trust between the Eindhoven police and city guards and its multi-ethnic inhabitants that visit Stratumseind late at night, there are likely more deeply imbedded issues standing in the way. For instance, certain minorities feel – sometimes rightly so – that they are unjustly targeted by the police and society more broadly.[39] As such, the level of trust in the police might not be very high (van der Leun, 2014). It is thus not unlikely that the *Trillion* app would mostly be used by those groups (often white Dutch citizens) that already have a sufficient level of trust in law enforcement and a distrust towards ethnic minorities. This might, in turn, lead to further inequalities between different societal groups (I discuss the particular privacy-related risks in Chapter 5).

While the project has officially ended, its results are not known to the public. In fact, most deliverables of the project were classified as confidential and the project's website is no longer in operation.[40] The *Trillion* app is no longer available in the Android Play store[41] and there is no news concerning the follow-up (if any) of the project in the news.

39 Police figures for Eindhoven in 2017 show that the proportion of registrations of discrimination in general based on land origin is greater than nationwide (van Bon, 2018). See also: Pieters, J. (2016, October). Dutch police excessively target ethnic minorities: report. NL Times. Retrieved from https://nltimes.nl/2016/10/03/dutch-police-excessively-target-ethnic-minorities-report.

40 See www.trillion-project.eu; accessed 23 March 2019.

41 Tested by the author on 8 November 2018.

5. CHALLENGES OF SMART CITIES AND LIVING LABS: IDEOLOGICAL RHETORIC, SOLUTIONISM AND NEOLIBERAL ETHOS

The promises of living labs and smart cities are tempting. With a lot of effort, time and luck, contemporary cities might indeed become more efficiently managed, competitive and sustainable with the help of technology. However, the realities of implementation of smart cities and living labs are messier and much more complex than the marketing materials of corporation and city managers say it is. Cities that capture, store, analyse and share large quantities of data also bring a number of social, political, ethical and legal concerns, as an increasing number of academic researchers (especially from urban geography) have pointed out (e.g. Edwards, 2016; Greenfield, 2013; Kitchin, 2015b; van Zoonen, 2016).

In preceding sections, I have examined the concepts of smart cities and living labs, identifying key characteristics of these initiatives. I have also closely examined an actually existing living lab in the Netherlands, gaining insight into its particular visions, implementations and struggles. In this section, I briefly set out the main challenges of smart cities and living labs as identified in urban and critical geography literature, including those of the *Stratumseind Living Lab* (*SLL*) in particular. While these challenges are very diverse, ranging from cybersecurity issues to a technocratic type of governance, I will focus on a broader range of issues that connect to the main topic of surveillance and privacy in public space (excluding those, which I address specifically in the following chapters, such as surveillance and the privatisation of public space). I will thus examine three types of challenges of living lab/smart city projects, which are also present in the *SLL*: ideological rhetoric, solutionism and neoliberal ethos. This discussion will enable me to discuss possible types and tools of regulation of surveillance within smart cities, particularly in relation to competition, communication and consensus, with more insight in Chapter 7.

5.1 Ideological rhetoric

The first set of issues concerns the ideological rhetoric of businesses and local governments that promises ahistorical, neutral and objective solutions, based on evidence or common sense, for problems of the city (Greenfield, 2013; Kitchin, 2015b). The smart city or living lab technology, including the data and algorithms, are portrayed as being objective and non-ideological, grounded in scientific experimentation or common-sense. The common claim is: sensors and cameras do not have agendas or politics, they simply measure light or count people. Likewise, the algorithms are portrayed as neutral and non-ideological, as its formulation and operation are said

to be grounded in scientific objectivity (Kitchin & Dodge, 2011). As such, they are supposed to produce readings and pictures that reflect the truth about the world. Such a framing enables these initiatives to present themselves as neutral, politically benign and common-sensical. Data urbanism (urban management based on data analytics) is presented as an inherently good thing, seeking to make cities safer, more secure, efficient, productive, sustainable and so on using data analytics.

However, technical systems do not exist independently of the ideas, techniques, technical components, people and contexts that conceive and produce them (Bowker & Star, 2000; Gitelman, 2013). Which data are generated and how they are analysed 'is the product of choices and constraints, shaped by a system of thought, technical know-how, public and political opinion, ethical considerations, the regulatory environment, and funding and resourcing' (Kitchin, 2014, p. 9).[42] Moreover, the data are generated within systems designed to enact a particular political and policy vision, resulting in data that are inflected by social values (and privilege). This holds especially within domains that function as disciplinary systems, such as law enforcement (Johnson, 2014). Smart technologies are thus thoroughly social and political and reflect the conscious and unconscious aims and biases of their designers.

These issues concerning ideological rhetoric can easily be seen in the *SLL* example. Firstly, the language of the *SLL* is daring. As follows from the interviews with the parties, there is talk about 'having guts', as such projects demand 'first getting things done and learning from mistakes later'. Moreover, the *CityPulse* and *De-escalate* projects promise that the technological systems will be able to detect the atmosphere and escalated behaviour on the street with the use of 'raw data', that is, objectively, and to prevent aggressive or criminal behaviour before it even occurs. Most of the promises of the *SLL* have also remained un- or under-developed within the official timeline of the projects. No predictive capabilities were developed within *CityPulse* and no measurable impact on de-escalation of behaviour within *De-escalate* was found. As such, these projects could be described as a success (at least, in terms of reaching their promises) only with difficulty. Failure in this sense is, of course, not problematic – one can learn just as much from bad examples as from good ones. Pilot projects, which are a way of applying new approaches in a confined field setting to learn about the innovation-context interaction, have been described to have a higher tolerance to failure (Vreugdenhil, Slinger, Thissen, & Rault, 2010). Instead, pilot project outcomes

42 This is not different in the case of very large sets of very diverse types of data (sometimes still called 'big data'). For a more detailed look into how 'big data' are not all-encompassing, exhaustive and politically benign, see Kitchin (2014).

provide input for learning. Clearly, pilot projects are closely connected to the notion of living labs, which also aim to provide such input. However, learning from failure (or mistakes more broadly) is not observed within the *SLL* (or other smart city initiatives examined in literature). There seem to be no evaluation reports, at least not available to the public or the author. In fact, the absence of any tangible success within the *SLL* does not seem not resulted in a change of operation or rhetoric within this and other similar projects. Quite the opposite, in local politics and media the *SLL* has been called 'an example for the rest of the country', especially in regard to resolving potential privacy issues ('Eindhovense innovatie is voorbeeld voor de rest van het land, staatssecretaris brengt bezoek aan Stratumseind,' 2018; translation by author).

5.2 Solutionism: a technocratic form of city governance

The second theme is a technocratic way of governing cities. This means that the emphasis is on creating technical rather than political and social solutions. This approach assumes that all aspects of a city (including safety, education, health and general prosperity) can be measured and monitored (also referred to as 'datafication'). As such, they are treated like a technical problem, which can be addressed through a technical solution (Kitchin, 2014, p. 9; Wiig, 2016). This is connected to what Morozov (2013) terms 'solutionism' – the belief that complex issues can be disassembled into neatly defined technical problems that can be adequately solved through technology. In other words, all that is required to understand, manage and fix the problems that a city faces, is a suitable technology, sufficient data and 'smart' algorithms.

Such thinking is based on a strong 'instrumental rationality' that privileges certain ways of thinking and doing over other forms of knowledge and action (Mattern, 2013). Employing a technological/algorithmic, thus evidence-based approach to city governance, seemingly ensures rational, logical, and impartial decisions (Kitchin, 2014, p. 9). This is an attractive approach to city management, as it provides the managers with a defence against decisions that raise ethical and accountability concerns by enabling them to say, 'It's not me, it's the data!' (Haque, 2012). Yet, this approach is actually highly narrow in scope and reductionist and functionalist in approach, as it is based on a limited set of particular kinds of data, failing to take account of the wider effects of culture, politics, policy, governance and capital that shape life in and of the city (Kitchin, 2014). It is clear, to many academics at least, that technological solutions on their own will not solve the deep-rooted structural problems in cities, as they do not address their root causes. Instead, they only enable (more or less) efficient management or optimisation of the manifestations of those problems. For example, a technological solutionist approach to aggression on the Stratumseind street is to produce an efficient aggression detection system that seeks to prevent (*CityPulse* project) or de-escalate (*De-escalate* project) it, or

to produce an app (*Trillion* project) that connects users to law enforcement in order to have them arrive on the scene of a problem earlier and identify the perpetrators more easily and quickly. These solutions do not address the more deeply engrained social and cultural issues underpinning aggression on the street or in Eindhoven more generally. As such, while smart city/living lab technologies are promoted as the *panacea* for tackling urban problems, 'they largely paper over the cracks rather than fixing them', unless they are coupled with a range of political/social, public policy and public investment initiatives (Cardullo & Kitchin, 2018).

Connected to technocratic governance is the critique of 'post-political' governance of the city (Vanolo, 2014). This approach to the management of cities and its citizens is said to mark a turn against the faith in liberal subjectivity, denigrating the place of older political processes in decision-making over infrastructure, and operating at a level beneath consciousness (Halpern et al., 2013, p. 291). This is so because smart city and living lab initiatives are increasingly becoming a generic and easily agreed upon target, without proper critical discussions and without 'politics', understood as the clash and debate between different ideas and positions (Vanolo, 2014, p. 891; cf. Gabrys 2014 writing about the re-articulation of citizenship in the contemporary smart city). Furthermore, Vanolo (2014, p. 889) talks about 'smartmentality', a discipline mechanism, where cities are made responsible for the achievement of smartness, in the sense of adhering to the specific model of a technologically advanced, green and economically attractive city, under pressure to obtain (European) funding and become involved in the marketing campaigns of private companies. Cities that choose to follow a different development paths are implicitly reframed as smart-deviant and depraved of institutionalised funding. Vanolo (*ibid*., p. 890) gives the example of southern Italian cities, facing more traditional urban problems, such as massive degradation of the historical centre, requiring physical improvement rather than any 'smart' transformation. However, in order to be a part of the 'smart' bandwagon, they are repositioning their problems according to the smart city discourse (in terms of ICT infrastructure, innovation, digital and entrepreneurial economy, flexibility of the labour market, the ability to transform) and, consequently, reorganising their agendas in directions that might not be the best for them.

This critique, at least in part, can also be applied to the *SLL* initiative and Eindhoven municipality, where policy documents reproduce the buzzwords and promises found in promotional materials of businesses selling the smart city/living lab 'solutions.' With this they open themselves up to such initiatives, with little or no discussion and little transparency. I discuss this issue further in Chapter 7 in connection to possibilities of regulation.

5.3 Neoliberal ethos

Connected to the post-political governance of cities, another common critique of smart city/living lab initiatives is that they are underpinned by a neoliberal ethos. These initiatives, at least in Europe and the U.S., are said to be the vehicle pushing the neoliberal agenda, thus leading to the corporatisation of city governance, further hollowing out the state and privatising the city service provision (Greenfield, 2013; Halpern et al., 2013; Hollands, 2008; Morozov & Bria, 2018; Townsend, 2013). The smart city and living lab agenda, it is argued, is overly driven by corporate interests, which are using these initiatives to capture government functions as new market opportunities. Big businesses offering smart city solutions, namely view city governance as a large, longer-term potential market for their products. Moreover, private actors invest in new data infrastructures in view of accessing and using 'public data', including the data that is captured through the monitoring of public space in return (Halpern et al., 2013, p. 282). City data is thus treated as a commodity. Beyond leading to the corporatisation of governance, this approach potentially creates technological lock-ins that tie cities to particular technological platforms and vendors over a long period of time, creating path dependencies and monopoly positions (Bates, 2012; Hill, 2013). From this perspective, the smart city is a 'one size fits all' approach, treating cities as generic markets and solutions that are straightforwardly scalable and movable, forgetting the specifics and contexts of each locale (including history, culture, politics and competing interests) (Kitchin, 2015b).

Such smart city solutions are thus said to be essentially an endeavour in creating markets for the very hardware, software and services on which these businesses are founded. In this sense, living labs (and smart cities more broadly) are test-beds for a form of urban life that is itself the product (Halpern et al., 2013, p. 290). This is so in a similar way that MacKenzie (2006) describes financial equations as 'engines, not cameras.' The same equations that are produced to model markets also produce the markets in the equations' very circulation. In a similar fashion, '[the smart city or the living lab] is an engine for urban growth even as it purportedly tests the capacities of its own infrastructure. In essence, it is an experiment that cannot end, because every limit becomes a new engineering challenge, a new frontier to develop toward an ever-extendable horizon' (Halpern et al., 2013, p. 291). A similar way of operation is found in relation to surveillance (see Chapter 2).

Even when there is the intention is to co-create with citizens in bottom-up, citizen-led projects with social impact (such as within in the European Commission's CAPS programme and the European Innovation Partnership for Smart Cities and

Communities – EIP-SCC),[43] many neoliberal structural obstacles exist. Although smart city and living lab initiatives are implemented at the local scale, their deployment and operation are strongly shaped by institutions operating on a higher scale, especially supra-national bodies, such as the European Union. Especially within the framework of EU funding of smart city projects that are supposed to be 'citizen-focused' (e.g. the *Trillion* project), there are many obstacles standing in the way of a truly citizen-focused initiative. Quite the opposite, smart cities that are conceived within this framework are said to enact a blueprint of neoliberal urbanism and promote a form of 'neoliberal citizenship' (Cardullo & Kitchin, 2018, p. 1). Cardullo and Kitchin (2018) have shown how the mechanisms of funding allocation, the application of scaling and replication techniques and mobile policy formation actively (re)produce a neoliberal conception of citizenship and participation. They have done so on the basis of the examination of smart city initiatives in Dublin, Ireland, finding that the various types of roles of 'smart citizens' are rooted either in 'tokenism' (informing or consultation with feedback; Arnstein, 1969) or, simply, non-participation (Cardullo & Kitchin, 2018, p. 2). This means that the citizen occupies a largely passive role, with businesses and city administrators performing forms of civic paternalism (deciding what is best for citizens) and stewardship (delivering on behalf of citizens).

In practice, citizen participation is often synonymous with 'choice' in the market, where the citizen is conceived as a 'user', selecting which services to acquire from the marketplace of providers, and a 'data product', creating data through her use of smart city technologies that companies can then incorporate into products and extract value from. Such a situation arises because the focus, objectives, and solutions are set *before* problems and suggestions from citizens can be taken into account. This should not be a surprise, if we look at how EU funding works. The consortium of multiple stakeholders applies for funding with a project proposal that is already designed to deliver specified outcomes. Only when it receives the funding do the stakeholders seek to engage with local communities. As Cardullo and Kitchin (2018, p. 9) put it:

> 'Any engagement that occurs after funding, even if designed to be citizen-centric, has then to meet pre-determined milestones and fulfil the deliverables of the contract, meaning citizens have limited scope to reframe the initiative around their concerns and desires.'

43 See European Commission. (n.d.). Smart cities. Retrieved March 19, 2019, from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

They use the example of the *Lighthouse* project (from the United Kingdom) aiming at reducing gas emissions in a city centre. Citizens, however, questioned the already established targets for implementing electric cars as a substitute for traditional more polluting cars, arguing for measures that would reduce the overall number of cars in the city and for an increase in green areas. Yet, due to the institutional lack of flexibility in such projects, their input could not be implemented nor seriously considered. This issue can also be observed in the EU funded *SLL* sub-project, *Trillion*. In this project concerned with community policing, the issue of anti-social behaviour on Stratumseind is attempted to be addressed by community policing via a mobile application, a goal which has been set before consultation with the general public. As such, other forms of activity that would tackle this issue and that visitors of Stratumseind (or inhabitants of Eindhoven in general) might prefer were not considered. Within the EU funded framework of smart city initiatives, citizens are thus at best encouraged to help provide solutions to practical issues of local implementation of the already chosen technological 'solution' (usually chosen by businesses in collaboration with the municipality). They are not encouraged to formulate or lead initiatives or propose communitarian projects, to draw an alternative to the fundamental political rationalities shaping issues, or to reimagine a political debate. In this sense, 'citizen-focused' is often just a buzzword to draw funding.

6. CONCLUSION

Living lab projects such as the *Stratumseind Living Lab* are already common practice in cities around the world and many more will be popping-up in the future. However, they are a relatively young research domain, lacking of a widely recognised definition and theoretical framework of the concept. The proliferation and growing importance of such projects, particularly in view of their promised societal impacts and role in creating contemporary life in the city, demands a more thorough analysis and disentanglement of the concept in order to uncover its substantial relevance in practice and problematic issues.

In this first Chapter, I have thus examined smart cities and living labs both from a theoretical as well as from a practical perspective. I have determined that the smart city generally refers to the extensive embedding of software-enabled technologies, particularly ICTs, into the city environment for two broad purposes: augmenting urban management and improving the quality of life in the city, on the one hand, and stimulating economic development of the city, on the other. Living labs, nowadays commonly found in connection to smart cities, refer to an experimentation

environment and a methodology for organising multi-stakeholder innovation processes, including users and communities of users, in a real-life setting, and aimed at the exploration, co-creation and evaluation of innovations. Connecting the ideas behind these two types of contemporary initiatives, we see that smart cities and living labs have a specific relationship. The deployment of living labs is, namely, said to represent a bottom-up approach to the smart city, designed to increase citizens' participation and involvement in solving local issues.

However, as follows from the *SLL* example and case studies done by other scholars (including the research into living labs in the Netherlands as done by the Rathenau Instituut), initiatives calling themselves living labs only rarely *actually* represent a bottom-up approach to the smart city. Quite the opposite, often such initiatives hardly involve citizens in the development of the project, especially in its earliest stages of identifying the issues and setting the means to go about solving them. Furthermore, smarty city and living lab initiatives (that is, the public and private actors behind them) favour technological solutions to societal problems, sometimes despite sound counter-arguments. As such, smart cities and living labs have been criticised for their ideological rhetoric, a technocratic form of city governance and a neoliberal ethos. These initiatives also lead to the privatisation and securitisation of public space (discussed in Chapter 4) and involve pervasive surveillance of such space (discussed in Chapter 2), leading to privacy concerns. The issues stemming from smart cities and living labs are thus very diverse and complex. In order to thoroughly analyse privacy-related risks stemming from surveillance within such initiatives, including possibilities for its regulation, insights from these various fields need to be brought together, possibly leading to a sum that is more than its parts. This first Chapter has thus offered the first set of insights, which form the foundation for further discussion in the following Chapters.

2

SURVEILLANCE THEORY
A chronological-thematic overview*

* This Chapter is largely based on a co-authored paper (Galič, Timan & Koops 2017) and a co-authored chapter (Timan, Galič & Koops 2017). The co-authors have granted me permission to reuse their work in this Chapter.

1. INTRODUCTION

As I have shown in the previous chapter, the entrepreneurial and the lay vision of smart cities and living labs is 'relentlessly positive', emphasising goals of sustainability, conviviality, democracy, and participation. Yet, these goals demand an intensive management of urban flows based on detailed data about ever more aspects of the city, including its people (Murakami Wood, 2015). The functioning of such 'smart' cities thus depends on digital technology – the sensor and network systems embedded in the infrastructure of the city, including video cameras, sound sensors, wifi tracking and nudging technology. This technology, used for detection of attributes, activities, people, trends, or events, however, also constitutes surveillance technology (Petersen, 2012, p. 10). Surveillance thus has a central place within smart city and living lab projects, so much that smart cities are often called 'surveillance cities' (Murakami Wood, 2015). This *other* side of the smart city as a surveillance city and its implications for human rights and community life, requires detailed analysis. In order to do this in more than a simplistic manner, however, one must get well acquainted with the particularities of the various types and logics of surveillance. This is what I attempt in this Chapter through a chronological-thematic overview of surveillance theory.

While surveillance was still considered 'little more than a prop for thrillers or science fiction movies' (Petersen, 2012, p. 7) in the mid-1990s, it has now become a household word. Yet there is considerable ambiguity as to the meaning of surveillance. Everyday uses and dictionary definitions of surveillance seem to capture only partially current realities of surveillance. Surveillance is commonly defined as 'close observation, especially of a suspected person' or as 'the act of carefully watching someone or something especially in order to prevent or detect a crime'.[45] However, most surveillance technologies today are not especially applied to suspected persons, but rather indiscriminately and ubiquitously, to everyone and in all contexts—all places, times, networks and groups of people (Marx, 2002, p. 10). Lyon, a key surveillance scholar, offers this definition: surveillance is 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction' (Lyon, 2007, p. 14), while Haggerty and Ericson (2000, p. 3) define surveillance as 'the collection and analysis of information about populations in order to govern their activities'. More broadly, surveillance can be described as a changeable 'mode

45 Following Oxford and Merriam-Webster online dictionaries.

of ordering' (Law, 1994),[46] responding to problems of government (Murakami Wood, 2013, p. 317). This means that surveillance does not function for itself alone but works to support other modes of ordering, which – in turn – can (and often do) generate and support the need for surveillance. A good example of this is the relationship between security and surveillance, where security is commonly used as a justification and a goal of the mass deployment of surveillance, both online and offline.

Surveillance is, of course, an ancient social process, but it is said to have become a dominant organising practice of late modernity over the past forty years (Lyon, Haggerty, & Ball, 2012, p. 1). Many surveillance scholars, thus, call our contemporary society a 'surveillance society' (e.g. Bauman & Lyon, 2013; Gilliom & Monahan, 2013; Lyon, 2001; Murakami Wood et al., 2006). The term 'surveillance society' generally refers to the fact that 'virtually all significant social, institutional, or business activities in our society now involve the systematic monitoring, gathering and analysis of information in order to make decisions, minimize risk, sort populations, and exercise power' (Gilliom & Monahan, 2013, p. 2). This development is best thought of as the outcome of modern organizational practices, rather than a type of covert conspiracy, as it is often presented in commentaries of surveillance practices (Murakami Wood et al., 2006). This also illuminates the two-sided, Janus-like nature of surveillance, which is both about caring and controlling (Lyon, 2006, 2007). The subject of surveillance is, namely, being watched with a certain purpose, which can be to control and discipline the subject into certain behaviour or a set of norms, but also – possibly at the same time – to protect and care for that subject. Surveillance is thus a phenomenon that is inherently ambiguous, highly dependent on context and complex social, technical and political arrangements. This ambiguity brings many risks stemming from visibility asymmetries and concrete possibilities to influence persons' behaviour brought about by surveillance.

As Newell (2018, p. 2) put it, 'public space has become a ripe and fruitful venue for surveillance of many kinds.' Public space is thus being transformed into increasingly observed and mediated space, largely in an unrestrained manner. This spread of surveillance, both in Europe and the U.S., generally follows from the vague idea that there is no or very little (right to) privacy in public space, especially where surveillance is seen as a means of fulfilling moral duties to protect and care for others (e.g. Himma, 2007). Surveillance is often seen as means of security and a solution to crime but

46 According to Law (1994, p. 83), modes of ordering are 'fairly regular patterns that may be usefully imputed for certain purposes to the recursive networks of the social [...] recurring patterns embodied within, witnessed by, generated in and reproduced as part of the ordering of human and non-human relations'.

one that also fits with a wider economic and political agenda connected to the contemporary restructuring of urban public space (Fyfe & Bannister, 1998, p. 257; I further discuss this in Chapter 4). In other words, surveillance is good both for security as well as for business. In this context, we have experienced an unprecedented spread of surveillance throughout the second half of the 20th century, both in the number and type of surveillance technologies, as well as the type and scope of persons and spaces being surveilled (Marx, 2002). This spread has not been overlooked in academia. Quite the opposite, it has triggered the emergence of a new scholarly discipline – surveillance studies. Surveillance studies is a multidisciplinary field (including perspectives of sociology, psychology, science and technology studies) covering both theoretical and empirical accounts of past, current and near-future surveillance in society. It deals with social changes in the dynamics of power, identity, institutional practice and interpersonal relations, examining what the role and effect of (particular types of) surveillance today is (Lyon, 2001, p. 4; Lyon et al., 2012, p. 1).

Situating the quick and messy surveillance developments in today's fluid and unsettling modernity (Bauman & Lyon, 2013) is not an easy task. On the one hand, most lay or policy commentaries still refer to Orwell's Big brother or Bentham's prison panopticon when talking about surveillance today.[47] But, as mentioned above, surveillance technologies and practices have changed significantly in the preceding decades, so that it is unclear whether these metaphors are still suited to describe contemporary practices of surveillance in public space. On the other hand, there is a deluge of diverging conceptualisations of surveillance practices, contemporary and historical, in surveillance scholarship. What is needed then, is a broad overview of stages and strands of theories and concepts of surveillance, in particular their key characteristics, goals and ways of functioning. Such an overview would namely enable a more structured identification of those concepts that are most relevant for the understanding of surveillance practices and its effects in contemporary smart cities and living labs that are the focus of this dissertation. In particular, it will enable me to identify specific surveillance practices (and their risks in relation to privacy) in the context of smart cities and living labs, using the example of the *Stratumseind Living Lab* (*SLL*), which I will do in Chapter 5.

This Chapter thus answers the sub-question, *how is surveillance conceptualised in prominent literature, particularly in surveillance studies?*

47 E.g. de Graaf, P. (2015, November 23). Een biertje met Big Brother erbij op Stratumseind. De Volkskrant. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/een-biertje-met-big-brother-erbij-op-stratumseind~b3cc767c/.

In this Chapter, I will thus examine historical surveillance models, paradigms and developments, offering a concise, chronological-thematic overview of key surveillance theories and concepts. The Chapter is structured as follows. In Section 2.1, I examine Bentham's Panopticons and Foucault's concept of panopticism and the disciplinary society – what I refer to as the first stage of the overview or 'architectural theories'. In Section 2.2, the second stage, I study more recent conceptualisations of surveillance by Deleuze, Haggerty and Ericson, and Foucault, which focus on networks, security and surveillant assemblages. I refer to these as 'infrastructural or post-panoptical theories and concepts'. Finally, in Section 2.3, the third and last stage of the overview, I explore contemporary piecemeal surveillance concepts, ranging from alternative -opticons to participatory surveillance and sousveillance.

2. SURVEILLANCE THEORY: A CHRONOLOGICAL-THEMATIC OVERVIEW

In this section, I offer a concise, chronological-thematic overview of surveillance theories and concepts, showing their development in time and focusing on the characteristics of current surveillance practices. I do so by discerning three stages: (1) 'architectural theories' – the Panopticon and panopticism; (2) 'infrastructural or post-panoptical theories' – control, surveillant assemblage and security; and (3) contemporary theories and concepts, each characterised by key features of a certain period and the technologies relevant for that time (in this I follow Galič et al., 2017; Timan, Galič, & Koops, 2017).

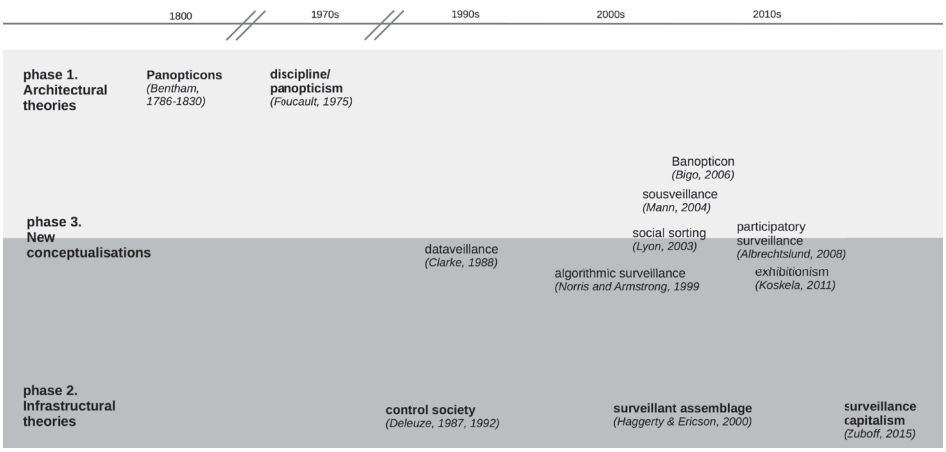


Figure 2.1: *A graphic of surveillance phases (Galič 2017, p. 34)*

2.1 Stage 1: 'Architectural theories' – the Panopticon and panopticism

2.1.1 Bentham's Panopticons

Although piecemeal theorization of surveillance occurred before the Panopticon, for example, regarding religious surveillance that dominated in the fifteenth century or political surveillance in the sixteenth and seventeenth centuries (Marx, 2002, pp. 17–18), I begin the first stage of surveillance theory-building with Jeremy Bentham and his panoptic designs from the end of the 1700s.

The Panopticon is probably Bentham's best-known but also most controversial idea (Schofield, 2009). It has become the most widely used metaphor for surveillance, becoming almost its synonym, so much so that many surveillance scholars today advocate forgetting the Panopticon when theorizing surveillance (e.g. Bauman & Lyon, 2013; Haggerty, 2006). The Panopticon has become particularly famous through Foucault's concept of *panopticism*, resulting in Bentham often being understood through the reading of Foucault. This, however, is misleading, and scholars are beginning to advocate that Bentham's thought be re-examined and the boundaries of well-established Foucauldian 'truths' about the Panopticon (which will be further explored in Section 2.1.2) be pushed back (Brunon-Ernst & Tusseau, 2012). In fact, scholarship has relatively recently come to the conclusion that Bentham did not create one Panopticon but at least four Panopticons.[48]

Besides, the well-known 'prison-Panopticon' (described primarily in *Panopticon; or the Inspection-House* (1786, 1790–1791)), there are also the 'pauper-Panopticon' (designed for the housing of indigents but also for reformation and work; described primarily in *Outline of a Work entitled Pauper Management Improved* (1797–1798)), the 'chrestomatic-Panopticon' (a Panopticon-shaped day-school, where one inspecting master could supervise pupils without being seen; described primarily in *Chrestomathia* (1816–1817)) and the 'constitutional-Panopticon' (although the term Panopticon is not used, the architectural arrangements are panoptic; described primarily in *Constitutional Code* (1830)). Foucault's concept of *panopticism* is primarily grounded on Bentham's description of the prison-Panopticon. However, the three less-known Panopticons do more than merely replicate the original prison-Panopticon idea; they present amended versions of the idea, reflecting its adaptation to new contexts and exemplifying different panoptic and even anti-panoptic features. Thus, Bentham uses 'the Panopticon' as a paradigmatic idea that can be adapted and used in a variety of social spaces and for different purposes.

48 Classification by Anne Brunon-Ernst (2012).

The prison-Panopticon depicts a prison designed as a circular building,[49] with an inspector in the central tower who oversees the activities of convicts in their cells. It is essentially an architectural idea, a 'strategy of space', but one that results in a 'new mode of obtaining power of mind over mind in a quantity hitherto without example' (Bentham, 2010, p. 15). Through specific architectural design, an illusion of constant surveillance is created—the prisoners are not really watched constantly but they believe they are. In Bentham's time, possibilities of surveillance were significantly bound by physical limitations. One of the key ideas or effects of the prison-Panopticon (and similarly designed Panopticons) was to create an extension of perception beyond visible locales and the reduction of temporal relations to spatial relations, thus enhancing the possibility of the disciplinary panoptic power (Božovič, 2010). Surveillance is carried out from one single point, and it is the inspector in his central lodge who possesses this extended power. The inspector is perceived as an invisible omnipresence, 'an utterly dark spot' (*ibid*., p. 11) in the all-transparent space of the prison-Panopticon, where the inmates are seen without seeing the one who sees them. It is precisely the inspector's apparent omnipresence that sustains perfect discipline in the prison-Panopticon—even a momentary exposure to the eyes of the prisoners would destroy the idea of his omnipresence in the minds of the prisoners. In the prisoners' perception, the inspector is all-seeing, omniscient and omnipotent.

This description of the prison-Panopticon is in line with Foucault's concept of panopticism, which theorises surveillance as involving an all-seeing inspector. Foucault defines panopticism as 'a type of power that is applied to individuals in the form of continuous individual supervision, in the form of control, punishment, and compensation, and in the form of correction, that is, the modelling and transforming of individuals in terms of certain norms' (Foucault, 2002, p. 70) where 'panoptic' refers to 'seeing everything, everyone, all the time' (Foucault, 2006, p. 52). But Bentham's vision, already in the prison-Panopticon, was not to create a 'society of control' where people would be watched all the time. Rather, the idea was that discipline would be internalised and the need for the inspector, the watching itself, would be eventually exhausted. This means that truly continuous and all-seeing inspection is not desired at all; in fact, already Bentham's prison-Panopticon was not actually all-seeing, and the purpose of such central inspection was to obviate the need for watching, punishment and the Panopticon itself.

49 Bentham later amended its shape to an octangular shape, whilst the pauper-Panopticon was dodecagonal (a twelve-sided polygon).

Bentham imagined the Panopticons as liberal political projects—they were proposed solutions to increasing social and economic problems of the time in Britain (e.g. in order to address the number of convicts and indigents that was rising fast beyond the state's capabilities) (see Schofield, 2009). According to his utilitarian philosophy, trying to achieve 'the greatest happiness for the greatest number of people', Bentham saw punishment as evil in itself, allowed only if it excluded greater evil. In regard to the prison-Panopticon, the specific architecture thus also served the goal of prisoners' liberation from more overtly coercive forms of institutional violence, which were common at the time. Moreover:

> 'the key point was not the fact that the inmates of Panopticon would be watched all the time, but … that they would be aware that they might be being watched. The inspector saw an infraction. He did not punish immediately, but waited. He saw a second infraction. At some point thereafter, he would confront the perpetrator with his record book. "See here, your infractions, with the date and time. This is your punishment." Once a punishment had been administered, and the prisoners saw that, should they misbehave, punishment was certain, they would no longer misbehave. There would no longer be any need for them to be watched. They would be reformed' (Schofield, 2009, p. 92).

There is more to Bentham's 'panoptic paradigm' (a term coined by Brunon-Ernst, 2012) than the authoritarian aspects of panoptic power described by Foucault. The panoptic paradigm as a whole, in the development of Bentham's philosophical and political thought, shows that the Panopticon is a more diverse and reversible structure than Foucault acknowledged. The Panopticon should be seen as a *template*, which can and should be adapted to the specific circumstances of other parts of society, in which methods of control are more complicated and accompanied by increasing exceptions to continuous individual supervision. In order to show how Foucault's panopticism fits less with Bentham's other Panopticons, the three less-known types will briefly be examined in the following paragraphs.

In the pauper-Panopticon, chronologically the second Panopticon and the most similar to the prison-Panopticon, specific circumstances demanded different treatment, leading Bentham to devise modifications to the building and management rules. The variety within the pauper population, consisting of all ages and coming from a wide variety of backgrounds and occupations, required a much greater degree of discrimination in treatment. Moreover, whilst prisoners were convicted criminals sent to jail by judges and magistrates, the paupers entering the pauper-Panopticon ('the industry house') did so voluntarily. Consequently, most paupers could leave the pauper-Panopticon whenever they wanted (although no one would enter a pauper-

Panopticon unless compelled by circumstances). However, according to the 'earn-first principle', no pauper would be fed and could not leave the Panopticon until he had completed his share of work (Schofield, 2009).[50] Also, children that were left in the pauper-Panopticon to be taken care of could not leave until they turned 17 (for girls) or 19 (for boys). On the other hand, certain groups of paupers were entitled to some privacy on certain occasions, by means of blinds that could be drawn across divisions (e.g. for marital sex, or seeking advice in certain situations from the 'Guardian Elders'- old paupers, supposedly immune to corruption due to their age, who constituted a type of additional 'inspectors' present in the paupers' rooms) (see Schofield, 2009). Nevertheless, the pauper-Panopticon still fits Foucault's panopticism well enough. In fact, due to specific circumstances demanding different treatment, the pauper-Panopticon involved more complex methods of control in some respects than the prison-Panopticon, such as surveillance done by the Guardian Elders and through book-keeping and rules on feeding and heating.

The third and fourth Panopticons have fewer panoptic features and even some anti-panoptic ones. The use of panoptic devices here is less clear than with the first two. The chrestomatic-Panopticon was a Panopticon-shaped school, where one inspecting master could supervise around sixhundred pupils per room without being seen. The plan was based on Bentham's 'scholar-teacher principle', whereby the more advanced pupils taught the less advanced, 'for the greatest improvement of the minds of students and the pockets of their parents' (Brunon-Ernst, 2012, pp. 21–23). Limits to panoptic control are more obvious here. First, panoptic control is exercised only whilst the children are in school; outside, they are out of reach of the panoptic gaze. Second, children were not assigned to a fixed class structure – they could change categories and classes in accordance with their age, subjects and level of achievement. Thus, specific forms of panoptic control upon them can also change.

Panoptic features are least obvious in the constitutional-Panopticon, devised only two years before Bentham's death. First, it is no longer the few watching the many but the many watching the few; citizens watch the governors (i.e. all those governing the citizens). The 'panoptic inspection principle' is thereby reversed, which is why certain scholars call this form of the Panopticon the *reversed* or *inverted* Panopticon

50 The idea was that they needed to 'earn back' the money spent for their upkeep, since the pauper-Panopticon, as all Panopticons, needed to be financially viable to serve as a solution to the social and economic problems of the time. Financial viability was a key challenge especially for the pauper-Panopticon and supposedly a key reason for Bentham ultimately to discard the idea of the pauper-Panopticon.

(Semple, 1987).[51] The focus is on governing functionaries, who are monitored through the use of more or less panoptic methods, to ensure they act in a way to maximise pleasure and minimise pain, or in other words, to prevent misrule. Second, as in the chrestomatic-Panopticon, the concept of constant visibility does not apply—the governors are monitored only in the course of their public duties, and they can withdraw from the citizens' gaze when they want to rest or enjoy some privacy. The term Panopticon itself is not used in the *Constitutional Code*; nonetheless, the architectural arrangements are panoptic. The position of the prime minister is at the centre of an oval-shaped building. Communication between the prime minister and his ministers, as well as between ministers themselves, is carried out (as in the other Panopticons) through communication tubes. Furthermore, each ministerial office is a thirteen-sided polygon, with a public or private waiting room on each side for people coming to visit the ministers. Although certain architectural designs remain in the constitutional-Panopticon, the central inspection tower disappears as artefact and as metaphor. Bentham believed that many places have become monitored because the people ensure good behaviour on part of their rulers through the instrument of publicity (transparency) (Schofield, 2009). In this, the newspaper has a key role, delivering information concerning misrule amongst the people and examining and criticising misrule (Kaino, 2009). Inspection (surveillance) is thus no longer central but rather dispersed. In Bentham's thought, the panoptic physical building, initially used strategically as a local architectural device, thus later becomes a universal monitoring tool in the wider project of ensuring good government.

It is primarily with the chrestomatic- and the constitutional-Panopticon that social control moves beyond the margins of society and focuses on its 'heart and head: middle-class children and members of the government' (Brunon-Ernst, 2012, pp. 27–28). The prison- and pauper-Panopticon could only reach the people inside the physical buildings with its panoptic control methods; people outside could only be reached with traditional, non-panoptic methods (using language and law, including deterring function). Non-marginalised people, thus, were beyond the panoptic gaze. Have the panoptic characteristics, then, increased rather than decreased in the last two Panopticons, which allow a wider gaze? That is not the case. Although the gaze embraced a much wider audience, it came with intentional limitations upon

51 Another example is Umberto Eco's pastiche of the *Anopticon*, a hexagonal building that effectuates 'the principle of 'being able to be seen by everyone without seeing anyone.' The *Anopticon's* subject is a prison guard who lives in a closed, central hexagonal room, unable to see anything other than a small circular portion of sky, and who is observed by the prisoners freely walking around in the corridors surrounding the guard's room (from Koops, 2010, p. 1035).

its panoptic power—it was not continuous and all-seeing. In the chrestomatic- and constitutional-Panopticon, the concept of constant visibility is reduced considerably: children were observed only whilst in school and the governors only when performing their public duties. Furthermore, in the constitutional-Panopticon, the gaze is reversed to oversee the rulers. Also, this is no longer done solely through architectural design but through dissemination of information in newspapers, as well. Of course, the news is still dependent on the architecture of the parliamentary building that enables the people to see what the government is doing. Here, the act of watching is no longer described in sinister terms such as central inspection, but in positive ones such as transparency and publicity.

These distinct features, some panoptic and others not, characterise what Brunon-Ernst terms Bentham's panoptic paradigm. The panoptic paradigm refers to Bentham's architectural projects operating as a model for governing the behaviour of individuals and groups and the operations of social practices or institutions and having the potential to function in non-disciplinary environments. This feature disqualifies the Panopticon as a uniquely disciplinary (in the Foucauldian sense) machine. This is so, since the Panopticons evolved more towards Foucault's concept of *governmentality* (Brunon-Ernst, 2012, p. 36), rather than towards disciplinary power through architectural design. Governmentality is, namely, a type of power—initially called security (*sécurité)* – different from discipline in that it no longer seeks to manage individual bodies but manages whole populations, trying to optimally regulate social behaviour (for a discussion of Foucault's security see Section 2.2.3). Bentham's Panopticons are devised in such a way that eventually no more Panopticons will be needed, and the panoptic age should be seen only as a stage in the transition to a non-panoptic utilitarian era, where misrule is minimised and pleasure maximised.

2.1.2 Foucault's panopticism and the disciplinary society

The first stage of surveillance theorisation continued with Foucault's concepts of panopticism and the disciplinary society and lasted until the end of the 1970s. Although Foucault's concept of panopticism is almost exclusively based on Bentham's prison-Panopticon, his analysis not only rehabilitated Bentham's work, but it also built upon and extended into a broader perspective on power relations and networks in modern societies (see further Galič et al., 2017).

Foucault projected the panoptical architecture of the prison-Panopticon as a diagram onto other parts of society in order to highlight power relations and models of governing (Foucault, 1991a). Through an analysis of different institutions, such as the school, the military, the hospital and the factory, processes of action in daily

life have been invaded with panoptical mechanisms of watching and being watched and, consequently, of disciplining power. When everybody can potentially be under surveillance, people will internalise control, morals and values—discipline is thus a type of power, a strategy and a kind of technology. In *Discipline and Punish*, Foucault offered a critique of the Enlightenment and showed that while liberation was preached on the level of (utilitarian) ideas, in practice, people were in fact subjects of new regimes of power—disciplinary regimes of a modern society with its progressively intensive organization and institutionalization (Dorresteijn, 2012, p. 50). Accordingly, he coined this type of society the disciplinary society, which (in the West) has seen a development towards technocratic approaches to governing. Therefore, Foucault shifted the perspective from the *goal* of governing to the *mode* of governing. The main goal is (still) to prosper as a society, delineated by geography or nation state. The *mode* of governance, however, has shifted from a sovereign society (seeking mainly to affirm control over a territory and securing the loyalty of subjects, in a somewhat static and rigid manner through binary prohibitions) (see Valverde, 2008) to one of discipline, which represents a shift in method as well as in object, from populations to individuals.

Disciplinary power produces a docile individual: 'out of a formless clay, an inapt body, the machine required can be constructed; posture is gradually corrected; a calculated constraint runs slowly through each part of the body, mastering it, making it pliable, ready at all times, turning silently into the automatisms of habit' (Foucault, 1991a, p. 135). Discipline thus represents a type of power working through normation and conformity. By this, he means the processes that force and create habits, rituals and how things are done, thereby create norms of behaviour.[52] In normation processes, the norm is central. It constitutes what one has to conform to and strive for; it is both standard and ideal. Being regarded as normal is to conform to the norm, hence to occupy the position of the invisible, i.e. unmarked by difference construed as abnormality, and putative universal subject. The abnormal is the one deemed deficient and inferior in relation to the norm(al) (Dalibert, 2014). This is specifically linked to the individual body, where discipline produces subjected and practiced, 'docile' bodies (Foucault, 1991b). In Foucault's understanding, normation is intrinsic to mechanisms disciplining the body, in which technologies are central (Foucault, 2007). Power (as discipline) then is becoming increasingly dispersed and hidden in

52 'The perpetual penalty that traverses all points and supervises every instant in the disciplinary institutions, compares, differentiates, hierarchizes, homogenizes, excludes. In short, it normalizes' (Foucault, 1991a, p. 183). See also Foucault (2007, p. 57), where he explains the difference between normation and normalisation.

processes of conformity. Although such power operates somewhat independently from the judiciary and government, it nevertheless requires institutions and the state, since it works *through* them – 'the state, correctional institutions, and medical institutions [need to] be regarded as coagulations of practices' (Valverde, 2008, p. 18).

Foucault continues that one *method* and a key indicator of disciplinary societies is found in many institutions that uphold and apply the norm: the exam. The exam incorporates the power of discipline because it tests according to a 'scientific' method the suitability of individuals against a norm. Through different methods of bureaucracy and sequences of how to do things, bodies get disciplined. For instance, the army applies extensive training and testing on using guns, hospitals on procedures of treatment and schools on writing and handling a pen *correctly.* The product or goal of these disciplining methods through the exam is to create docile bodies, which become units of information (e.g. so many students passed the exam and so many failed). This makes societies more susceptible to prediction and planning.

Here, the link becomes clear with Bentham's prison architecture: it is a one-way street in which individuals are mouldable and re-mouldable.[53] Modernity then, in the form of disciplinary societies, is formed by the advent of scientific methods of registration, record-keeping and normation through exams. Docile individuals are no longer governed as actors with whom they communicate, but as units of information that can be moulded. Surveillance is a key concept here because this moulding and re-shaping is a result of the visibility of individuals' 'competencies' through exams and record-keeping of their progress. Foucault briefly mentions, but does not elaborate upon, resistance to disciplining power, by stating that the entanglements of power also give rise to scattered points of resistance that have no cause but power itself, which they resist (Foucault, 1998).

The above leads to a way of thinking and applying the concept of the prison-Panopticon as a metaphor to describe a phenomenon that has been coined *panopticism*. In relation to the rise of CCTV cameras, for example, Foucault's analysis of a methodical and objective observer holding disciplining power resonated very well. Indeed, the watcher cannot be seen, and there is a constant (mediated) gaze that, like the watcher in the watchtower, *might* see everything. Normation and internalisation of 'doing good' are achieved through cameras, and citizens in public space can thus be moulded into behaving according to the norm. The footage can be stored, allowing the watcher to

53 'The Panopticon was also a laboratory; it could be used as a machine to carry out experiments to alter behaviour, to train and correct individuals' (Foucault, 1991a, p. 203).

be 'omnipresent' not only in space, as in Bentham's prison design, but also in time. CCTV seemed the perfect example to prove Foucault's analysis being spot-on, which might help explain the wide resonance of his theory. However, there are features of CCTV and other forms of electronic surveillance for which the Panoptical model cannot account, simply because under the influence of ICT, society and its institutions have changed radically from those in Foucault's analysis. I will examine these in the following Sections.

The characteristics of surveillance, as emanating from Foucault's concepts of discipline and panopticism, thus correspond to a great extent with Bentham's prison-Panopticon. In conclusion, the main characteristics of the 'architectural' or panoptical stage in surveillance theory are:

(1) surveillance is mostly physical, confined to closed physical spaces, and visible; although, because of the way disciplining power works, surveillance became more dispersed and less visible with Foucault than it was in Bentham's Panopticon;
(2) the main actor of surveillance is the state with its institutions;
(3) the object of surveillance is the underclass (although the focus is becoming broader with Foucault's conceptualisation) where the focus is on individuals and their physical bodies;
(4) surveillance aims at discipline; and
(5) surveillance is mostly perceived as negative and sinister, although certain positive or empowering aspects are also recognised.

2.2 Stage 2: 'Infrastructural theories' – networks, surveillant assemblages and security

The second stage of surveillance theories begins in the late 1970s with the rise of (consumer) capitalism as a global political system and the emergence of computers and subsequently networked technology as household appliances. This stage is 'post-panoptical' since its representative authors tried to get away from the Panopticon as the primary model for thinking about surveillance, arguing that surveillance has transformed into something different due to changes in the socio-technical landscape (e.g. Haggerty, 2006; Lyon, 2007). This section thus features authors who try to develop alternative theoretical frameworks to the Panopticon as the primary model to conceptualise surveillance in modern Western societies. Deleuze, the founding father of post-panoptical literature, attempted to find places of surveillance analysis beyond the Panopticon already in the late 1970s and through the 1980s. Deleuze (sometimes together with Guattari) located new places of surveillance in a physically and technologically changed environment – networks. Haggerty and Ericson look

particularly at new combinations of humans and technology that exercise forms of surveillance. The last author that I will examine in this Section is, again, Foucault. In his lectures from the second half of the 1970s, he tried to get away from his ideas of the disciplinary society, conceptualising what he initially called 'security'. These authors thus challenge the units of analysis in the works of Bentham and Foucault, arguing that new analytical tools are needed, and they therewith establish a post-Panoptic or 'infrastructural' stream of surveillance theory.[54]

2.2.1 Deleuze's control society: from governments to companies

Deleuze observed that Foucauldian institutions and their ways of disciplining no longer existed, or at least were shifting into other modes of surveillance and exercising power. Partly in collaboration with Guattari, he further developed the shift, already described to some extent by Foucault, from disciplinary societies towards societies of control (Deleuze, 1992; Deleuze & Guattari, 1987). These authors diverge from panoptical thinking by proposing a series of new places of power in order to conclude that the socio-technical landscape has changed. Especially in the short but high-impact piece 'Postscript on the Societies of Control', Deleuze specifically dismisses the idea of discipline as a goal or driving force of 'governing'; rather, it is now found in forms of control.

Deleuze considers how the driving forces of capitalism and globalisation are changing (Western) societies and how institutions such as the school, the hospital or the factory have become corporations. The difference from the disciplinary society lies both in the process and the method. Where discipline aims to achieve a long-term, stable and docile society striving for the optimal use of resources to reach government-issued goals, corporations focus on more short-term results. In order to do so, they need constant control, and this is achieved through continuous monitoring and assessment of markets, workforces, strategies, etc. The corporation is a fundamentally different *creature* than the nation-state, because it does not strive for progress of society as a whole; it tries instead to control certain specific parts of – increasingly international – markets (Taekke, 2011, pp. 451–452). To illustrate, the point is not to create a good and steady carpenter, but to know how and where to put a nail in a piece of wood as efficiently as possible. The carpenter has therefore become a *coded figure* of

54 Another stream of post-panoptical theories and concepts could be examined here, namely, Zuboff's neo-Marxist perspective on surveillance – 'surveillance capitalism' (Zuboff, 2019). As this perspective on surveillance, focusing on the emerging logic of capital accumulation in the online world, fits less well with my focus on surveillance in physical space, I leave it out of my analysis. For an overview of this idea, see Galič et al. (2017).

corporation (Deleuze, 1992), which means that his skills could be valuable one day, but, as markets change, useless the next. This is called *modulation* (*ibid*., p. 2), where systems or institutions are constantly changing and thereby also changing the fibres of society. These modulations take place in ways that are mostly invisible for the subjects or citizens. Where discipline for Foucault was effective because of its visibility and its active (although involuntary) participation – you have to work/pass the exam/ abide by rule X – Deleuze states that modulations happen in invisible and opaque networks that are unperceivable to individual citizens. As a result, surveillance moves away from being a present and often physical force on individuals, to become more abstract and numerical:

> 'The disciplinary societies have two poles: the signature that designates the *individual*, and the number or administrative numeration that indicates his or her position within a *mass*. This is because the disciplines never saw any incompatibility between these two, and because at the same time power individualizes and masses together, that is, constitutes those over whom it exercises power into a body and moulds the individuality of each member of that body. […] In the societies of control, on the other hand, what is important is no longer either a signature or a number, but a code: the code is a password, while on the other hand disciplinary societies are regulated by precepts' (Deleuze, 1992, p. 50 emphasis in original).

Surveillance has also become more opaque and widespread. It is no longer the underclass that captures the attention of surveilling actors, but 'productive citizens', who are increasingly being constituted as primarily or merely consumers, leading to the creation of consumer profiles with the intention of moulding their purchasing behaviour. It is no longer actual persons and their bodies that matter and that need to be subjected and disciplined, but rather the individuals' representations. It is the divided individual – consumers and their purchasing behaviour – who has become important to monitor and control. Deleuze (1992) coins this the *dividual* (a divided individual) – 'a physically embodied human subject that is endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems' (Williams, 2005). For Deleuze, networked technologies have made it clear that individuals, 'discrete selves', are not in-divisible entities; on the contrary, persons can be divided and subdivided endlessly. What starts as particular information about specific people is thus separated from us and recombined in new ways outside of our control (*ibid*.). Such 're-combinations' are based on criteria deemed salient by those with access to the information, both governments and corporations. For example, one can be divided for one purpose as a consumer and a citizen and, for another, as an Albert Heijn customer or a Jumbo customer.

Where society is becoming fragmented, so is the individual, who is split up into pieces, with the power of consumerism demanding all kinds of attention from citizen-consumers. In a Deleuzian society, it is thus no longer individuals as wholesome beings and their physical bodies that are of interest to surveillance, but the representation of parts of individuals from data trails: their data doubles (Poster, 1990). The Deleuzian notion of the dividual directs the gaze not towards individuals as complete or uniform beings, but rather towards individuals as entities with many roles, represented in many different places (data-banks). Surveillant visibility is no longer directly applied mainly to individuals but to flows and movements. Such flows and movements are not only or mainly material but concern primarily money, choices, attentions and habits, all projected into the monist dimension of information (Brighenti, 2010b, p. 162). As a result, surveillance now focuses on the construction of consumer profiles in order to limit or control access to places and information and to the offering or refusal of social perks, such as credit ratings or rapid movement through an airport.[55]

Where Foucault studied closed spaces and enclosed institutions, such as the factory, the prison or the hospital, striving to make individual bodies docile, Deleuze focuses on open spaces and points attention to control at a distance, using technologies of power that reform bodies (and minds) through daily regimes instigated by those in power. Power has thus taken a shift towards controlling *access*. Consequently, Deleuzian places of interest are airports and borders, as access points (something taken up in later surveillance conceptualisations, see Section 2.3.1). Simultaneously, control ceases to be the exclusive prerogative of the state and becomes scattered and disseminated throughout plurality of social sites and locales (Lyon, 2007).

2.2.2 Haggerty and Ericson's surveillant assemblage

Deleuze's incredibly early insight to networks of power and the decoupling of individuals' bodies and their representations served as a main inspiration and source for more recent surveillance scholars. Haggerty and Ericson (2000) developed one of the most important and widespread contemporary conceptualizations of surveillance in their seminal paper 'The surveillant assemblage'. Although their concept of surveillant assemblage goes somewhat beyond post-panoptical theories and shares certain characteristics with what can be called the third stage of surveillance theories,

55 In this sense, Deleuze (1992, p. 7) mentions Guattari's imagined city 'where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position—licit or illicit—and effects a universal modulation.'

it fits best in the second stage, as their theory is firmly rooted in a post-panoptical view of society and Deleuzian-Guattaresque concepts: assemblage and the rhizome (see Deleuze & Guattari, 1987).

Assemblages can be defined as a 'multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they *work* together as a functional entity' (Haggerty & Ericson, 2000; Patton, 1994). Beyond this functional entity, with a stability only on the surface, assemblages comprise of discrete flows of an essentially limitless range of phenomena, such as people, signs, chemicals, knowledge and institutions. These fluid and mobile flows become fixed into more or less stable and asymmetrical arrangements – *assemblages*, visualised as devices hosting opaque flows of auditory, olfactory, visual and other informational stimuli. These assemblages turn into systems of domination allowing someone or something to direct or govern actions of others; the inevitability of transformation is key to thinking in terms of assemblage (Murakami Wood, 2013). Surveillant assemblages can hence be seen as 'recording machines', since their task is to capture flows and convert them into reproducible events. Haggerty and Ericson used this concept, because they identified contemporary surveillance to be emergent, unstable and lacking discernible boundaries or accountable governmental departments, so that it cannot be criticised by focusing on single, confined bureaucracies or institutions. Such surveillance is driven by the desire to bring systems together, leading to an increased convergence of once-discrete systems of surveillance and an exponential increase in the degree of surveillance capacity.

The authors also described surveillance as rhizomatic, another concept taken from Deleuze. Rhizomes are plants that grow in surface extensions through horizontal underground root systems, a way of growing that differs from arborescent plants, which have a deep root structure and grow through branches from the trunk. This means that surveillance is growing and spreading increasingly in unlimited directions, working across state as well as non-state institutions, by rhizomatically expanding its uses (for purposes of control, governance, security, profit, and entertainment), particularly with the help of new and intensified technological capabilities, relying on machines to make and record discrete observations.

Rhizomatic surveillance can consist of multiple parts, aspects, and agents that do not necessarily share similar intentions or goals. Surveillance thus can no longer be seen as relatively stable and physically controlled but as a malleable, fluid and unstable phenomenon, perceptible to people as multiple surveillant assemblages (control networks/circuits or 'Little sisters'; Romein & Schuilenburg, 2008, p. 347). In

other words, surveillance has become de-territorialised, operating as a heterogeneous network of elements and spreading rhizomatically. Although this can have a somewhat levelling effect on hierarchies of surveillance and result in new categories of people being monitored (and even in bottom-up surveillance), surveillance continues to play an important role in establishing and reinforcing social inequalities, and the primary focus is still on creating profit for corporations and the state (see also Romein & Schuilenburg, 2008). These new characteristics of surveillance fit well with the idea of a control society replacing the disciplinary society (at least, as the main mode of ordering), in which citizens are no longer subject to disciplinary or simple repressive modes of surveillance in confined spaces (with power as an element of the interior of separated spaces); rather, citizens are being increasingly constituted as (merely or primarily) consumers 'seduced into the market economy'. Hence, surveillance today is used increasingly to construct and monitor consumption patterns (rather than perform 'soul training'), constructing consumer profiles in order to, as Deleuze and Guattari already pointed out, limit access to places and information, leading to the offering or refusal of social perks.

Social control within the surveillant assemblage is, thus, decentralized and shape-shifting. As such, monitoring is often directed towards the human body for the purpose of canalising access to places and information and allowing for the production of consumer profiles through the *ex post facto* reconstruction of people's behaviour, habits and actions. Such surveillance takes place in two consecutive steps: de-territorialisation and re-assembly. The body is first broken down, abstracted from its physical setting, only to then be re-assembled in different settings through a series of data flows. The result is a decorporealised body, more mobile and measurable than its physical counterpart, re-assembled in a 'data double' (Haggerty & Ericson, 2000, p. 611). The data double, however, goes beyond representation of our physical selves – it does not matter whether the double actually corresponds to the 'real' body. The data double constitutes an additional self, a 'functional hybrid' (Hier, 2003, p. 400), serving foremost the purpose of being useful to institutions, which allow or deny access to a multitude of domains (places, information, things) and discriminate between people. The doubles flow through a host of scattered 'centres of calculation' (e.g. forensic laboratories, statistical institutions, police stations, financial institutions and corporate and military headquarters) in which they are re-assembled and scrutinised for developing strategies of administration, commerce and control. The chief idea is that from all the data that people generate in daily behaviour (using credit cards, browsing the Internet, using smartphone applications, working, travelling, walking on the street, etc.), profit *should* be made. Nevertheless, Haggerty and Ericson also briefly point out that surveillance can be seen as a positive development, offering

possibilities for entertainment, pleasure, even (to a limited extent) resistance to top-down surveillance and power over the powerful (see also Haggerty, 2006). While this point still mainly serves as an afterthought in the second stage, it becomes a more prominent point in the third stage (see Section 2.3).

2.2.3 Foucault's security

In the second half of the 1970s, Foucault no longer saw discipline as the main organising principle of modern society. In his 1978 lectures, titled 'Security, territory, population', he claimed that the fundamental aspect of government at the time was 'security' (*sécurité*). With this term he referred to future-oriented management of risks through the management of entire populations, in particular territorial configurations. At the beginning of the fourth lecture, however, Foucault changed the term 'security' into 'governmentality'. As Valverde (2008, p. 29) eloquently put it:

> 'frustratingly for governmentality scholars, he does not explain why he changed terms. He simply walks in one day (February 1, 1978) and declares that if he were able to go back and correct the theme and title of that year's lectures, he would no longer use the advertised title, "Sécurité, territoire, population," but rather "Lectures on governmentality." Then he goes on to talk about techniques of governmentality, with security quietly receding into the background.'

Following several established commentators of this part of Foucault's scholarship (including Bigo, 2008; Dilts & Harcourt, 2008; Klauser, Paasche, & Söderström, 2014; Valverde, 2008), I will continue to use the term 'security' here, as it better fits more recent trends of connecting surveillance with the goal of 'security' (leading to interesting connections between 'surveillance studies' and 'security studies'[56]). Among the key rationales for engaging in surveillance, a key motif today is procuring 'security', an ill-defined and incredibly broad term (Bauman & Lyon, 2013, p. 100). Nevertheless, security is a political priority today in many countries and a massive motivator for the spread of surveillance (Zedner, 2009). For the purpose of this Chapter, I will restrict my analysis of 'security' as used by Foucault and will not delve into an analysis of governmentality and biopolitics, as done by several other scholars (see, for example, Dean, 2010).

The concept of security reflects Foucault's critical understanding of capitalism and liberalism. According to him, the discourse of liberalism did not fall in contradiction

56 This is an interesting and relevant topic to examine, however, it goes beyond the scope of this dissertation.

to governmental practices, rather, it allied itself with them. He saw liberalism not as anti-governmental but as expressive of a governmental rationality (Brighenti, 2010b, p. 153). Whereas in the disciplinary and policing model of the *ancien regime*, the emphasis was on the unseen seeing eye of the guardian, including the police (present everywhere without being seen whilst knowing that we might always be observed), in security practices the ideal shifted towards policing as the activity of seeing the invisible; in other words, of visibilising social processes and making them legible (*ibid*., pp. 153-154). The aim was to enhance the visibility and, *a fortiori*, the order. Furthermore, while security is a necessary complement of liberty, as it secures liberty (being future oriented and risk driven), in the modern liberal society, security has also become an end in itself and, thus, a means for the suppression of liberty (Valverde, 2008, p. 28).

Security is future-oriented and has a resource-maximisation logic (*ibid*., p. 23). Its key aim is risk management, for example in relation to public health. As such, security does not prohibit anything, rather it incentivizes certain economic activities (while discouraging others). It is tied to the arts of minimising and maximising (Harcourt, 2014, p. 4) – to the competence of economists who try to reach an equilibrium point for populations as a whole, also engaging in cost-benefit analysis. Security is, thus, centrifugal (in opposition to discipline, which is centripetal) – it is tolerant of minor deviations and seeks to optimize, to minimise or maximise, rather than eliminate. If discipline conforms and uniforms, security selects and sorts. Moreover, security does not refer to a single apparatus. Foucault talked about assemblages of security (*le dispositif de sécurité*), which comprise of sets of technologies the general aim of which is to govern multiplicities in open spaces on the basis of actuarial devices (Brighenti, 2010a, p. 60).

On the one hand, discipline tries to control enclosed places and single bodies, that is through individualisation. Disciplinary normalisation thus consists in breaking down a given multiplicity (e.g. of people or behaviours) into specific components (Foucault, 2007, pp. 56–57; Klauser et al., 2014, p. 873). On the other hand, security aims to control open spaces and irreducible multiplicities. Such multiplicities cannot be pinned down to the individual level, so security cannot be applied to individuals. Instead, security focuses on the relationship between components of a given reality (Foucault, 2007, p. 47), including a focus on space and organising it according to a series of *possible events* that are to be managed and kept under control. In order to do so, it conceives and organises space as an abstract concept, a system of possibilities, of virtualities that do or do not become actual (Welch, 2008). 'Spaces of security' (Foucault, 2007, p. 11) respond to the need to regulate, optimise, and manage circulations. In practical terms,

in order to ensure security, open public spaces thus need to provide mechanisms for surveillance whereby authorities can monitor the comings and goings of the floating population, for the general purpose of 'optimised adjustment of the assembled components of reality' (Klauser et al., 2014, p. 873). Since an expanding town is oriented towards the future, security measures are put into place in order to ensure its prosperous well-being.

> 'In other words, it was a matter of organizing circulation, eliminating its dangerous elements, making a division between good and bad circulation, and maximizing the good circulation by diminishing the bad. It was therefore also a matter of planning access to the outside, mainly for the town's consumption and for its trade with the outside' (Foucault, 2007, p. 18).

Whereas discipline aims to govern a multiplicity of subjects by impacting them directly (*singulatim*), upon individual bodies (in order to control them, train them, make them conform to the norm), security governs the multiplicity as an *omnes*, an undivided whole (Brighenti, 2010a, p. 60). As explained in Section 2.1.2, the norm in discipline works by 'normation'. In contrast, security works by 'normalisation'. In other words, within the disciplinarian framework people are classified by reference to a norm, setting apart the normal from the abnormal. In the securitarian framework, however, people are treated as an undivided whole, where the issue is one of operating an aggregate, statistical, or average normalised management of biological processes such as nutrition, health, and so on (*ibid*., p. 60). The apparatus of security, thus, 'lets things happen within the limits of the acceptable, whilst also regulating and monitoring them with a view to the optimisation of reality in its intertwined components' (Klauser et al., 2014, p. 874). Therefore, security does not postulate a perfect and final reality to be achieved, rather it is a constant process of optimisation derived from and taking place within a given reality, whose aims are constantly readapted and redefined, depending on the (ever)changing parameters of reality and the shifting context and conditions of regulation (e.g. cost calculations, public opinion, availability of novel control techniques; *ibid*.). As such, the normative logic of Foucauldian security is fundamentally flexible in its management of reality. In this, the operation of security comes very close to that of modulation (see Section 2.2.1).

The object upon which security is exercised is, thus, the *population* – a global mass, a collective and statistical concept, which could be termed the 'data double of society'.[57] The population 'exists only as a pattern within a grid of dimensions and variables,

57 I would like to thank to prof. Koops for suggesting this term.

which include "impersonal" events such as birth, death, production, reproduction, and illness' (*ibid*., pp. 60-61). The population has no will, so it is not 'a people' in the classical political-philosophical sense, nor an actor in the sociological sense. It just shows certain *tendencies* that must be normalised. Technologies of security therefore try to control aggregate tendencies without shaping them from within.

Connections between Deleuze's control model of power and Foucault's security have been pointed out by several scholars (e.g. Brighenti, 2010a; Murakami Wood, 2013; Puar, 2012). It can be said that in both conceptualisations, surveillance is exercised in the open space of the public domain and is focused on a 'population' which is regarded and scrutinised *qua* 'dividual' information flows (Brighenti, 2010a, p. 65). While some scholars have gone so far so as to claim that Deleuze's concept of control society and Foucault's security are the same (Murakami Wood, 2013, p. 319; Puar, 2012), there certainly are visible connections between the two. Foucault's conceptualisation of surveillance as 'security' thus fits well enough in the second stage of surveillance theories. The main characteristics of corporate-networked and security theories of surveillance, therefore, are:

(1) surveillance is abstract, numerical, reproductive (widespread and ever-spreading), and often invisible or opaque;
(2) the main actors of surveillance are corporations; even when performed by state institutions, these act as corporations;
(3) the object of surveillance is, both, a *dividual* – specific parts of an individual deemed useful to corporations and as discerned from their data doubles, as well as whole populations and multiplicities;
(4) surveillance aims at controlling access and managing flows, seeking to optimise; and
(5) it is perceived in a mainly negative way, although certain positive aspects of surveillance, including possibilities of resistance to it, are acknowledged as well.

2.3 Stage 3: Contemporary piecemeal surveillance concepts

The third and latest stage in surveillance theory, which covers contemporary concepts of surveillance, is characterized by a branching out of theories in different directions, building on previous theories but focusing more on particular phenomena within surveillance than on building all-encompassing theories (Galič et al., 2017). This differentiation and particularization in conceptualisation can be connected to a steady increase in, but also diversification of, surveillance devices, data sources, actors, use contexts, and goals, and, consequently, more and varied forms of surveillance. The surveillance industry has grown rapidly since 9/11, both in size and in type. It is a

fitting continuation of the trend Haggerty and Ericson started to map out. The pace of technology development and its use is now so rapid and unpredictable that surveillance theories and concepts oftentimes remain piecemeal and need to be regularly revisited. In fact, there is no attempt (perhaps no need) to build an overarching theory, as the main surveillance theories in the first two stages did.

The roles of the watcher and the watched along with power relations in society are becoming more and more diffuse, particularly as the dedicated surveillance technologies are increasingly intertwined with mundane and accessible consumer technologies. Where the first two stages clearly distinguish between surveillance objects and subjects, the third stage develops into a much messier affair. On the one hand, there is an increasing blend of governmental and corporate surveillance infrastructures that make use of commercial, mundane, and accessible tools such as laptops and mobile phones to collect consumer/citizen data. This form of surveillance is less obvious and visible than the physical infrastructures of the first stage. On the other hand, an increase of citizen-instigated forms of surveillance can be witnessed, in which the same laptops and mobile phones are equipped with cameras. Consequently, with the heightened presence of cameras, the act of making pictures, movies, and other forms of media creation in public and private spaces is increasingly becoming standard practice. The recording and sharing of all kinds of human activity through digital platforms adds an entertaining and pleasurable aspect to surveillance, and challenges (but does not replace) existing power relations of surveillance in society.

Thus, the third stage is characterised by particular surveillance concepts or *diagrams* (Elmer, 2003) studied in specific contexts or case studies. The three most notable contemporary surveillance concepts, comprising contemporary piecemeal surveillance theory, are alternative *-opticons*, participatory surveillance and *sousveillance*, which I examine bellow.

2.3.1 Alternative –opticons

Despite the search for post-panoptical theories since the end of the 1970s, the Panopticon is still often used as a metaphor to analyse surveillance in current technological contexts. David Lyon states that 'we cannot evade some interaction with the Panopticon, either historically, or in today's analyses of surveillance' (Lyon, 2006, p. 4). The metaphor might indeed still be valid due to an ever-growing presence of 'watching and being watched' mechanisms through various new (ICT) technologies. Where the second (infrastructural) stage emphasized the virtual, representative layers of surveillance through databases, Lyon would argue that the disciplining power exercised through the Panopticon as described by Foucault is still present: it merely

shifted from the physical architectural prison that corrected inmates, through the workplace and government for reasons of productivity and efficiency, to current, 'softer' forms in entertainment and marketing. Through reality shows and YouTube, 'to be watched' is becoming a social norm, even an asset – the more views the better. Lyon calls it 'panopticommodity' and Whitaker the 'participatory Panopticon' (Lyon, 2007; Whitaker, 1999). Both try to capture and project ideas of watching and being watched as a form of discipline onto current, contemporary manifestations of what basically is, they claim, the same panoptic principle.

Similarly, Latour argues, with his concept of an 'oligopticon', that panoptic principles are still in place, yet dispersed via smaller sub-systems and situations – a network of multiple smaller *Panopticons* that all have a different disciplining power on individuals (Latour, 2005). Each of these *Panopticons* has its own particular gaze and its own methods and related technologies through which it operates. The partial vantage points of the Oligopticon, however, are increasingly linked as databases are connected. Moreover, 9/11 brought about a rapid growth of (Deleuzian) surveillance as control, for example in the form of access gates or checkpoints that citizens now encounter in daily life. In an attempt to conceptualize this event and what it did to notions of control, freedom, and security, Bigo (2006) coined the concept of the BANopticon, which, instead of monitoring and tracking individuals or groups to identify misbehaviour, aims at keeping all bad subjects out: it bans all those who do not conform to the rules of entry or access in a particular society. He points out that a series of events, most prominently the 9/11 attacks, have declared a 'state of unease' and an American-imposed idea of global 'in-security' (*ibid*., p. 49), leading to what Agamben (2005) calls a permanent state of exception or emergency. This leads to a rhetoric of 'better safe than sorry' under which surveillance measures are expanding to what is sometimes called 'blanket' surveillance, in which every nook and cranny of society would seem under observation. This rhetoric is recurring when new and experimental surveillance technologies enter parts of society. Importantly, in this rhetoric frame one cannot be 'against' surveillance.

2.3.2 Participation and empowerment in surveillance

Another development considered to have a long-term effect on surveillance structures is the Internet. New media and surveillance scholars argue that the ways in which we govern life have rigorously changed because of it. Connected to Internet infrastructures of databases, servers, and screens, other driving forces and events emerge that change the legitimacy and reach of surveillance in society. Partly through the lens of the Internet, scholars look for other than us-versus-them perspectives on surveillance. Following Haggerty (2006), more positive and empowering accounts might be found

in systems of watching and being watched. If we accept that we indeed live in some form of a networked and technology-saturated society, it follows that apparatuses of surveillance, the methods, tools, and technologies already mentioned by Foucault are not solely in the hands of top-down and power-hungry governing institutions or governments. Even if we follow Deleuze's reasoning that corporations are now in charge with a surge for power and control that is even more threatening because of their opaqueness and invasiveness, the individual can still resist, refuse, or find alternative ways of using technology. Due to an increased blending with consumer technologies, mainly through ICT, surveillance technologies have become increasingly accessible to ordinary citizens.

Instead of being a place where one looks at many, most social media technologies follow the logic of 'many look at many', where visibility is often deliberately chosen. In that vein, Albrechtslund (2008) in particular diverts from solely negative concepts of surveillance. Rather, he argues that since the emergence of ubiquitous computing, surveillance as a concept should be re-considered. 'The entertaining side of surveillance is a phenomenon worth studying in itself, and we expect that this type of study will contribute to an understanding of the multi-faceted nature of surveillance' (Albrechtslund & Dubbeld, 2005, p. 3). Albrechtslund looks at how surveillance is often used as a design principle in, for instance, online games and sports-tracking services. Besides a fun aspect, such games and services can also inform us about how a (part of) society reflects on notions of surveillance. Albrechtslund coins the term 'participatory surveillance' in order to illustrate how citizens/users are both actively engaged in surveillance themselves as watchers, but they also participate voluntarily and consciously in the role of the watched.

Many online environments, especially social networking sites (boyd & Ellison, 2008), serve as interesting places of study, since many beliefs, ideas and opinions are shared there. boyd and Ellison (2008) even state that social networking sites are dominating online activities today and as such, they constitute new arenas for surveillance. From the perspective of users and visitors of these online places, the high level of surveillance, in the form of tracking and being tracked, watching and being watched, or sharing and being shared, is not necessarily negative:

> 'Characteristic of online social networking is the sharing of activities, preferences, beliefs, etc. to socialize. I argue that this practice of self-surveillance cannot be adequately described within the framework of a hierarchical understanding of surveillance. Rather, online social networking seems to introduce a participatory approach to surveillance, which can empower – and not necessarily violate – the user' (Albrechtslund, 2008).

Participating through, for instance, sharing, responding or 'liking' engages users into these platforms, where the idea of being seen and 'followed' is a precondition rather than a setback. This is also referred to as self-surveillance, a term that, with recent technological trends such as mobile healthcare applications (*m-* or *e-Health*) and wearable computing, resonates more and more. The added value of this concept is that it allows for a user-centred perspective on surveillance, rather than a top-down or institutional analysis. Following boyd (2011) and Marwick (2012), this approach enables another type of analysis of surveillance, where tracing behaviour can reveal users' experiences of surveillance and visibility. Concerning the question, why visibility is so important to these users, Koskela (2011) for instance explains that exhibitionism such as shown on social networking sites or in TV shows can work in an empowering way. By throwing everything into public arenas, 'visibility becomes a tool of power that can be used to rebel against the shame associated with not being private about certain things. Thus, exhibitionism is liberating, because it represents a refusal to be humble' (Koskela, 2004). Similarly, in the marketing context, Dholakia and Zwick argue that ultra-exhibitionism

> 'is not a negation of privacy but an attempt to *reclaim some control over the externalisation of information*. As such, ultra-exhibitionism is to be understood as an act of resistance against the surreptitious modes of profiling, categorization and identity definition that are being performed by others on the consumer whenever he or she enters the electronic "consumptionscape"' (2001, p. 13; emphasis in original).

A counter-argument to the empowering view of (self-)surveillance, however, is that emerging forms of self-tracking, in for example mHealth or other measurement apps, in combination with participation as a design principle could be seen as a facade or illusion of self-control, where actually users are being tracked and traced in the background. From a neoliberal point of view, one can also interpret self-tracking and self-surveillance apps as the ultimate model of 'nudging' (Thaler & Sunstein, 2009), in which governments, institutions and companies are pushing back responsibilities (for health, for instance) onto individuals (J. E. Cohen, 2016). In this sense, the way power operates is no longer enforcement and punishment but, rather, through temptation and seduction. It is moving away from normative regulation to public relations (PR) management, from policing to the arousal of desire (Bauman & Lyon, 2013, p. 57). In a way, this view re-introduces the Panopticon as a fitting metaphor – we are not only internalising doing good via external influences of (partly digitised) institutions in surveillant assemblages, but we are also, through self-monitoring apps and other forms of participatory surveillance, internalising these rational models and methods in a self-induced process of self-disciplining. Furthermore, this logic points to a type of

society that Bauman (*ibid.*, p. 27) called a 'confessional society', in which we experience no joy in having secrets. In this society, privacy is 'invaded, conquered and colonized the public realm – but at the expense of losing its right to secrecy' (*ibid.*, p. 27). In such a society, those who care about their invisibility are bound to be rejected, pushed aside, or suspected of a crime.

Another type of participatory surveillance is found in vigilantism, such as public vigilance campaigns related to policing. While vigilantism is not a new phenomenon (it can be traced back to witch hunts in 14th century Europe; see Larsen & Piché, 2009, p. 188), it has experienced an expansion at the end of the 20th century due to new possibilities of digital technologies. As Larsen and Piché (*ibid.*, p. 196) put it, '[d]oing vigilance is foremost a way of watching others and interpreting behaviours and appearances.' Vigilantism is thus a type of participatory surveillance, where citizens watch other citizens in order to further certain goals, such as policing in the case of community-based crime prevention groups (see e.g. Johnston, 1996; Trottier, 2018). We could also say that citizens are transformed into 'citizen-spies' (Monahan, 2006) or 'Little Brothers' (Larsen & Piché, 2009), thus linking this type of surveillance to the new types of -opticons. This practice, however is said to fail in yielding useful tips to law enforcement, while reproducing the general culture of racial profiling and leading to additional opportunities for exclusion and 'othering' (Larsen & Piché, 2009, p. 197; Monahan, 2006). This is largely due to the vague message of such campaigns, so that citizens need to rely on common-sense understandings of what constitutes suspicious or undesirable behaviour. The public is thus encouraged to trust their knowledge of what a 'normal' citizen ought to look and act like. Of course, what constitutes suspicious abnormality is informed by particular narratives that circulate in the public sphere. For instance, in the context of contemporary terrorist attacks, suspicious abnormality is mostly found in connection to ethnic, racial, and religious characteristics (e.g. Giroux, 2005; R. Jackson, 2005). As such, vigilantism also offers new opportunities for exclusion and 'othering', often reproducing the general culture of racial profiling (Ball, Timan, & Webster, 2019; Larsen & Piché, 2009; Monahan, 2006). While public vigilance campaigns address and involve the public, they do so in an atomised and individualised manner, inviting and fostering suspicion towards others and thus contributing to the dissolution rather than constitution of community (Larsen & Piché, 2009, p. 201).

2.3.3 Sousveillance and other forms of resistance

Another conceptual axis along which surveillance in the third stage is analysed, concerns the level and type of resistance that is possible and present in certain contexts. Although the logic of sharing in new media has its own economic drivers,

recent developments do hint at another possibility that this democratization of (surveillance) technologies offers—namely to perform acts of counter-surveillance. One concept that emerged in the early 2000s is Steve Mann's 'sousveillance' (Mann, 2004), a mode of monitoring in which citizens watch governing bodies from below, as an opposing concept to *sur*veillance (watching over or from above). Due to an increased availability of camera equipment and other recording devices, Mann argues that one form of resistance is (and should be) to 'watch back' at those who watch us. Where Mann uses the example of wearable cameras to watch back at CCTV cameras, the idea of sousveillance could also be transposed to the digital or the virtual context, where citizen journalism and publishing (leaked) information about surveillance actors can be seen as forms of watching back. Also, in the context of analysing processes of social sorting and exclusion, it can prove insightful to look into forms of resistance and sousveillance to investigate whether and how individuals and groups resist current forms of surveillance, dataveillance and surveillance capitalism. As end-users of social media, as feeders of 'big data' or as 'implicated actors' (Clarke & Montini, 1993) of CCTV or wifi tracking, people still have some room for negotiation and resistance – for 'anti-programs' (Latour, 1999) in use. Examples are citizens who choose to avoid CCTV cameras in cities (Brands & Schwanen, 2014), wear anti-surveillance-drone hoodies, use a special browser like Tor that provides a high level of anonymity, install free software (like 'Detekt') that detects spyware on your computer or feed faulty data into algorithms.

Although surveillance studies sometimes offer such practical cases and techniques to dodge surveillance (for example M. Roessler, 2002), conceptualisations of resistance or 'pushing back' are as yet quite scarce. This might be connected to two asymmetry problems: first, an asymmetry of power, since we rarely get to choose whether or how we are monitored, what happens to information about us and what happens to us because of this information; and second, an asymmetry of knowledge, since we are often not (fully) aware of the monitoring and how it works at all (Brunton & Nissenbaum, 2013). These two asymmetries can reinforce our lack of resistance, since how can we resist something that we do not understand, know about and often simply can hardly influence?

A notable exception is the concept of 'obfuscation', made particularly prominent by Brunton & Nissenbaum (2013, 2015). They provide tools and a rationale for evasion, noncompliance, refusal and even sabotage, particularly aimed at average users who are not in a position to 'opt out' or exert control over their data, but also offer insights to software developers (to keep their user data safe) and policy makers (to gather data without misusing it). They invoke the notion of 'informational self-defence' in

order to define obfuscation, which they see as a method of informational resistance, disobedience, protest or covert sabotage to compensate for the absence of other protection mechanisms and which aids the weak against the strong (Brunton & Nissenbaum, 2013). Obfuscation in its broadest form thus 'offers a strategy for mitigating the impact of the cycle of monitoring, aggregation, analysis and profiling, adding noise to an existing collection of data in order to make the collection more ambiguous, confusing, harder to use and, therefore, less valuable' (*ibid.*, p. 169). They offer wide-ranging examples, from 'quote stuffing' in high frequency trading to the swapping of supermarket loyalty cards. Many obfuscation tools, such as Tor and proxy servers, are however still not widely known or deployed outside the relatively small circles of the privacy-aware and the technologically savvy; moreover, they come with transaction costs (e.g. Tor can be slow and is blocked by many large websites). They also discuss certain ethical and political scruples (Brunton & Nissenbaum, 2013; Mercer, 2010; Pham, Ganti, Uddin, Nath, & Abdelzaher, 2009) to indicate that obfuscation is not a panacea to address the downsides of surveillance. Nevertheless, Brunton and Nissenbaum see obfuscation as both a personal and a political tactic and therewith offer a theoretical account of resistance that can serve as a platform for further studying legitimate and problematic aspects of surveillance and its opposition in an age of ubiquitous data capture.

These piecemeal contemporary developments in surveillance conceptualisation can be seen as a way of situating surveillance developments in the fluid and unsettling modernity of today, where surveillance spreads in hitherto unimaginable ways. As Bauman and Lyon (2013, p. 3) put it, 'surveillance spills all over'. The main characteristics of contemporary theories and concepts of surveillance hence are:

(1) surveillance is physical as well as abstract and numerical, it is confined and open, stable and liquid, visible and opaque;
(2) the main actors of surveillance are the state, corporations, and individuals themselves;
(3) the object of surveillance is both the 'productive' citizen and the underclass, both individuals' physical bodies and dividuals and data doubles, both individuals and groups;
(4) surveillance aims at both discipline and controlling access; and
(5) it is perceived as sinister as well as beneficial and even entertaining.

3. CONCLUSION

In this Chapter, I have offered a rough chronological-thematic overview of surveillance concepts and theories in the form of three stages: panoptical, post-panoptical and contemporary piecemeal theories and concepts of surveillance. I have done so in order to provide a more structured insight into the various forms of surveillance. As already mentioned, we are experiencing a steady increase in, but also diversification of, surveillance devices, data sources, actors, use contexts, and goals of surveillance. Surveillance is found not only in governments monitoring people's online communications (most prominently revealed by Snowden) or in businesses tracking our online shopping patterns (for example, through the use of cookies and loyalty cards) but also in our own actions of posting personal videos and pictures on social media, through which we willingly contribute to our own surveillance. In other words, surveillance comes in all shapes and sizes. As such, it is important to have a good foundation for discussion and further development of the field.

The first phase, featuring Bentham and Foucault, revolves around the Panopticon and panopticism. It can be characterised as offering architectural theories of surveillance, where surveillance is largely physical and spatial in character, either in concrete, closed spaces or more widespread in territorially based social structures, and largely involves centralised mechanisms of watching over subjects. As such, panoptic structures are theorised as architectures of power – through panoptic technologies, surveillance enables power exercise, not only directly but also, and more importantly, through self-disciplining of the watched subjects.

The second phase moves away from panoptic metaphors and shifts the focus from institutions to networks and to relatively opaque forms of control. This phase can be characterised as offering infrastructural theories of surveillance, where surveillance is networked in character and relies primarily on digital rather than physical technologies. As such, it involves distributed forms of watching over people, with increasing distance to the watched, often dealing with data doubles rather than physical persons or with multiplicities (e.g. algorithmic groups) rather than individuals. A common theme to the different accounts of Deleuze, Haggerty and Ericson, and Foucault, is the question how to conceptualise the power plays in contemporary network societies beyond panoptic effects of self-disciplining.

In the third phase, we find surveillance theory building on, and sometimes combining insights from, both theoretical frameworks of the first two phases, to conceptualise surveillance through concepts or lenses of dataveillance, access control, social sorting,

peer-to-peer surveillance and resistance. With the datafication of society, surveillance combines the monitoring of physical spaces with the monitoring of digital spaces. In these hybrid surveillance spaces, not only government or corporate surveillance is found, but also self-surveillance and complex forms of watching-and-being watched through social media and their paradigm of voluntary data sharing.

Most importantly for the purpose of this dissertation, I have tried to show in this overview that choosing a surveillance framework through which to analyse a particular type and context of monitoring matters. An analysis of surveillance within the *SLL*, for example, through the lens of the prison Panopticon, surveillant assemblage or Foucault's security will shed very different lights and thus raise very different implications for human rights and community life.

While the above chronological-thematic overview might seem to suggest that the proposed stages are succeeding each other (just as capitalism replaced feudalism, for instance), this is not the case. Quite the contrary, they represent modes of power that continue to exist alongside each other, but in particular times, places and contexts one of them comes to be the dominant operational logic (Brighenti, 2010a, p. 64; Harcourt, 2014, p. 11; Sadowski & Pasquale, 2015). As Bauman (in Bauman & Lyon, 2013, pp. 55–56) put it:

> 'the panopticon is alive and well … but it has clearly stopped being the universal pattern or strategy of domination both [Bentham and Foucault] believed it was in their times; it is no longer the principal or most commonly practised pattern or strategy. The panopticon has been shifted and confined to the "unamanageable" parts of society, such as prisons, camps, psychiatric clinics and other "total institutions".'

These modes of power are not at all incompatible (Murakami Wood, 2013, p. 319). While many scholars have made claims that we find ourselves today in a post-panoptic surveillance society (including distinguished surveillance scholars like David Lyon), one might better state – following Bauman – that the panopticon is still 'alive and kicking' but alongside other, more prevalent, modes of power.

These insights are noteworthy, especially if we are to take surveillance studies from books to practice. This is precisely what I try to achieve in Chapter 5, in which I examine the particular shapes and sizes of surveillance taking place in smart cities and living labs, using the example of the *Stratumseind Living Lab*, and the privacy-related risks stemming from them. The above overview will enable me to connect the specific actors, types of technologies and goals of the three examined *SLL* sub-projects

(*De-escalate*, *CityPulse* and *Trillion*) to the fitting types and functions of surveillance, the dominant mode(s) of power involved, and, finally, the risks that such surveillance poses for privacy in public space. In order to do this, I will employ the identified general characteristics of the three stages as I have identified them in this Chapter:

(1) what are the general characteristics of surveillance: is it physical, confined and stable, or numerical, networked, open and liquid?
(2) who are the main actors of surveillance: the state, corporations or individuals themselves?
(3) who is the object of surveillance: the underclass, the productive citizen, individuals or groups, the individual physical body or dividuals and data doubles?
(4) what is the aim of such surveillance: disciple, control or anything else?
(5) is surveillance perceived as sinister, beneficial or even entertaining?

Before I can do this, however, I need to examine the concept of privacy, both from a theoretical as well as a legal perspective. This is needed as privacy is a notoriously ambiguous and contested concept and right, rather than a straightforward notion, as is often presumed in surveillance studies and other disciplines. As such, the concept of privacy and rights to privacy need to be thoroughly examined on its own. This is what I do in the following chapter.

3

KEY THEORETICAL PERSPECTIVES ON PRIVACY AND THE RIGHTS TO PRIVACY

1. INTRODUCTION

Scholarly research into privacy and the right to privacy began properly in the 1960s and 70s in Europe and the U.S. (e.g. Miller, 1971; Rodotà, 1974; Westin, 1967), largely as a reaction to the emergence of computerised databases, wiretapping and psychological testing, and its implications for our private lives (e.g. Igo, 2018). However, despite decades of prolific research, privacy is still seen as a very complex, multi-faceted concept. Solove (2008, p. 1) calls it 'a concept in disarray'. And as Igo (2018, p. 10) states, it can be 'amusing, if also sobering, to come across other observers' frustrations with how ungovernable [the subject of privacy] is.' But privacy has also been described as complex in positive terms. Hildebrandt (2006b, pp. 50, 53), for instance, describes it a 'fruitful indeterminacy' and a concept 'too complex and rich to be defined in strict terms'. Mulligan, Koopman and Doty (2016, p. 3; following Gallie 1956) have called privacy 'an essentially contested concept', where disputes about its core are both paramount and central to the concept itself (as, for instance, with 'democracy', 'art' or 'freedom'; Gallie, 1956, p. 149). Rouvroy and Poullet (2009, p. 50) have described the right to privacy as having an 'intermediate value' or a 'tool' (serving other values and rights), thus granting plasticity to relevant laws and ensuing their ability to meet the evolving challenges of ICTs and society more broadly. In this sense, privacy can also be seen as a 'fundamentally fundamental right' (Burkert, 2008) – a necessary precondition to the enjoyment of most other fundamental rights and freedoms.

However, what we perceive as complexity is not entirely inherent in phenomena. On the contrary, the perceived complexity of a situation depends in part on how well we can simplify reality in a coherent way (King, Keohane, & Verba, 1994, pp. 9–10). In this Chapter, I attempt to make sense of this complex concept for the purposes of examining privacy in public space by deconstructing it into several more manageable pieces that can offer additional insight in this broken-down form. As a consequence of this approach, some insights on privacy and the rights to privacy will end up being of more use for this purpose than others.

In this sense, I posit that a part of the confusion and somewhat exaggerated claims of complexity that surround privacy is at least partially connected to the fact that the term 'privacy' is used to refer not only to a legal right (the various aspects of privacy protected by law, including the human right to respect for private life and the right to protection of personal data) and a concept (rather, various conceptualisations of privacy) but also to a socio-behavioural phenomenon (private life). All of these *privacies* are of course heavily connected and interdependent, but they also differ in significant ways, each developing in its own manner and having different implications. It is important

to distinguish between these in order to adequately understand this complex notion and, particularly, to avoid the common conflation of the legal concept of privacy with the broad philosophical, political, and psychological concepts of privacy (Rouvroy & Poullet, 2009, p. 52). For instance, not every violation of the concept (or sense) of privacy is necessarily a violation of the right to privacy, as this right – like all legal protection – is not absolute (Hildebrandt, 2006b, p. 46). Yet people, including legal scholars, like to talk about privacy as if it were a uniform concept, which can lead to various misinterpretations and confusion. In this Chapter, I will hence break apart these three *privacies* (the right, the concept, and the phenomenon), enabling me to get a better grasp on the concept of privacy that can inform both the right(s) to privacy as well as the concept of privacy in public space.

The aim of this Chapter then is to identify the underlying values, types and mechanisms in privacy theory in order to inform the conceptualisation of privacy in public space. The research sub-question that I try to answer is: *how is privacy – both as a phenomenon, concept and as a set of legal rights – conceptualised in general, especially in Europe?* This will enable me to later determine whether these generally identified values, dimensions and mechanisms of privacy broadly fit, warrant and enable the protection of privacy in public space or whether other conceptualisations should be created (see Chapters 5, 6 and 7). As Rouvroy and Poullet (2009, pp. 49–50) have claimed, identifying the values in which the right to privacy finds its roots provides contemporary scholars (as well as lawmakers and courts) confronted with new developments of surveillance technologies with more solid objectives against which to assess the adequacy of current legislation and propose reasoned improvements.

Furthermore, the focus of this Chapter (as of the dissertation in general) is on scholarly discussions of privacy in Europe, particularly continental Europe. As explained in the Introduction, this is so because its conceptualisation and discussion in Europe (unlike in the U.S.) is very much connected to the established fundamental and human right status of privacy, particularly as stemming from Article 8 (the right to respect for private life; discussed in Chapter 6) in the European Convention of Human Rights (Koops et al., 2017; Rouvroy & Poullet, 2009, p. 48). The *existence* of the right to privacy (or private life) is thus not debated; what is debated, however, is its scope and the underlying values. Nevertheless, since the U.S. debate on privacy is influential also in Europe (Koops et al., 2017; also seen in the often invoked 'reasonable expectation of privacy' standard), this Chapter will inform and enrich its discussion also with insights from authors across the pond.

The Chapter is structured in three main sections. First, I try to 'make sense' of privacy by examining the phenomenon or practice of privacy and the philosophical foundations of the modern concept of privacy. Second, I examine the concept of privacy by distinguishing the value of privacy, privacy dimensions and mechanisms for attaining privacy. Finally, in the third section, I examine the development of the *rights* to (or law of) privacy (excluding data protection, for reasons explained in the Introduction), focusing on the particularities of its development in continental Europe. First, I offer a brief history of the rights to privacy, beginning with Roman law. After that I focus on contemporary conceptions of rights to privacy, including a brief description of Warren and Brandeis' right to be let alone, an examination of personality rights, the spheres theory and, finally, the human and fundamental right to privacy (or private life).

2. MAKING SENSE OF PRIVACY: A BRIEF ACCOUNT OF PRACTICES AND PHILOSOPHICAL FOUNDATIONS OF PRIVACY

2.1 'Privacy before privacy': from the phenomenon to the philosophical foundations of the concept

2.1.1 Privacy as a socio-behavioural phenomenon

According to Perrot (1990, p. 1), some still describe privacy as an experience of the present (or at least modern) age. While this claim might indeed hold for privacy as an idea or a concept, privacy as a socio-behavioural phenomenon, a practice, seems to have always existed, even if to varying degrees.

There is ample evidence that people in all societies (both Western and non-Western) have always practiced some form of *private life*. Virtually all societies namely have techniques for setting distances and avoiding contact with others in order to establish *physical* boundaries to establish privacy, such as concealment of genitals, seclusion during birth or death, the preference for intimacy during sexual intercourse and restricted entry into homes by non-residents. And although some cultures appear to show no concern for privacy in regard to changing clothes, birth, death and even excretion (what is typically considered most private in Western societies), anthropologists have found that these cultures use various *psychological* methods for achieving privacy for the individual or the family when communal life makes physical privacy impossible (DeCew, 1997, p. 12).

Murphy (1984), for instance, writes about the use of the veil for providing social distance, as a way to establish and maintain social relationships (both intimate and not) among the Tuareg people in northern Africa. Geertz (1959; as described in Westin, 1984, pp. 64–65) compares household-privacy practices in two Indonesian societies, Bali and Java. According to him, in Java native people live (or still lived at the time) in small, bamboo-walled houses, where non-family members wander in freely and very little physical boundaries existed from the outside world. The result is that their defences – acquiring a sense of privacy – were mostly psychological. Relationships even within the household were thus very restrained – people spoke softly, hid their feelings and behaved with full decorum as if in public even within the home. In contrast, houses in Bali were surrounded by high stone walls, entry was possible by a narrow, half blocked-off doorway and non-family members hardly ever entered the house-yard. In the Balinese house, warmth, humour and openness were found.

Moreover, Westin (1984; cf. Hall 1966) pointed out that humans are not the only species on the planet that has a need for privacy. According to him, virtually all animals seek periods of individual seclusion or small-group intimacy (*ibid*., p. 56). These territorial patterns are said to serve a cluster of important purposes, including ensuring the propagation of the species by regulating density to available resources, enhancing selection of 'worthy' males and providing breeding stations for animals that require male assistance in raising the young (*ibid*., p. 57). In fact, ecological studies have shown that animals have minimum needs for private space without which the animal's survival will be jeopardised.[58]

It is thus by now a well-established claim that although the practices and rituals of privacy vary across cultures and time, every society acknowledges the normative importance of privacy in some form (J. L. Cohen, 1997, p. 156; More, 1984). Privacy then can be said to be a cross-cultural and even cross-species universal phenomenon (DeCew, 1997, p. 12).

2.1.2 The development of (Western) private life

The realm of private life, understood in the sense of a gradual and continuing development of social, familial and personal relationships, interests or activities, which are distinct from the public or professional aspects of life, is not something given in nature. Rather it is a historical reality, construed differently by different societies in

58 Experiments with spacing rats in cages showed that even rats need time and space to be alone (E. T. Hall, 1990, pp. 21–29).

different times, and it is a slowly constituted realm (Ariès, 1989, p. 3).[59] Historical and anthropological literature document the increased physical and psychological opportunities in societies to gain privacy through economic autonomy, mobility and other developments (DeCew, 1997, p. 13). In this Section I will briefly examine the most influential account of the history of private life in Western society, based on vast historical, anthropological and ethnological research focused on France and England, that has been done by Philippe Ariès et al. in their influential five-volume *A history of private life*.

According to Ariès (1989, p. 3), private life makes sense only in relation to public life. Furthermore, a key redefinition of the boundaries between private and public life occurred after the 15th century (*ibid*., p. 1). The individual in the late Middle Ages in Europe was enmeshed in feudal and communal life, moving within the limits of a world that was neither public nor private. The individual's 'private' life was confounded with its 'public' life as he or she deeply depended on the community or a certain patron (for more see Elias, 1978).[60] As Ariès (1989, p. 9) put it: 'A person has nothing that he or she could call his or her own – not even his or her own body. Everything was in jeopardy, and only willingness to accept dependency ensured survival.' Under such conditions the public and private clearly could not be differentiated. The situation started to change in the 15th century, when a person's life began to develop separate private and public parts. This development, according to Ariès, is linked to three fundamental changes. The first is found in the new role of the state beginning in the 15th century, when it started to assume responsibility for certain governmental functions, such as maintaining law and order, courts of law and the army (*ibid*., p. 10). The second big change is seen in the Protestant Reformation and the Catholic Counter-Reformation of the 16th and 17th centuries, which apart from encouraging more collective forms of parish life, demanded a greater inward piety and more intimate forms of religious devotion (Catholics primarily through confession and Protestants through keeping private diaries). The third major event can be found in the progress of literacy and an increased availability of books with the development of the printing press in the 15th century. This development enabled individuals to emancipate themselves from the community and the culture based on speech and gesture, by allowing the reader to

59 As such, I should emphasise that my intention in this brief excursion into the development of private life in Western Europe is not to present this development as an inevitable result of the development of civilisation. Rather, I try to present it as a particular cultural-historical reality following the most accepted account of the phenomenon to date.

60 Hans-Peter Duerr (in his four volumes of 'Der Mythos vom Zivilisationsprozeß'), however, has argued against Elias, claiming that there has always been some form of distinction between private life and public life. As his claims are only marginally accepted in academia, I will not discuss them.

develop and retreat into a solitude of the mind, opening up possibilities for solitary, gregarious and family activities (Chartier, 1989b, p. 15).

These developments thus allowed for the creation of a closed private realm, autonomous and divorced from the public service, to which the individual could retreat, when he needed refuge from the community (Y. Castan, Lebrun, & Chartier, 1989, p. 111).

Ariès suggests a possible periodization of this development from the 15th throughout the 19th century in three phases. The first period, beginning in the 15th century, represents a period of heightened individualism in daily life (although not in ideology), when the individual began to set himself apart from the collectivity. In the second period, in the 17th and 18th century, individuals *escaped* their newly created solitude by joining together in small groups of their own choosing (smaller than the village, neighbourhood, class or guild, but larger than the family). And, finally, in the third period, in the 19th century, the private sphere shrunk so that it coincided with the family unit, which became the primary centre of intimacy and emotional investment (Chartier, 1989a, p. 399). The family was no longer a merely economic unit for the sake of whose reproduction everything needed to be sacrificed, rather it became a refuge to which people fled in order to escape the scrutiny of outsiders and an emotional centre (Ariès, 1989, p. 8).

In the 19th century, the family and the familial home, thus, represented the locus of privacy (Hunt & Hall, 1990, p. 87), so much so that the family became almost synonymous with private life. However, prior to developments in housing after 1950, individuals (except for the wealthy few) enjoyed privacy at home only in common with others who shared the same living space. Domestic privacy was thus 'nothing more than the public space of the household' (Prost, 1991, p. 62). Sexual activity, for example, was either relegated to the semi-public realm (such as the woods behind a dance hall or a thicket at the edge of a field) or exposed to view or hearing at home. Gradually, however, the individual succeeded in establishing new rights (both in the sense of social claims and legal rights), partly in opposition to the family, partly with its support (Castan, Aymard, Collomp, Fabre, & Farge, 1989, p. 447). The 'private' in the 20th century finally began to represent withdrawal in two senses, thus defining the essence of privacy in the modern era: first, representing withdrawal from the public sphere, civic responsibility and the affairs of the city or state; and second, representing withdrawal from the family, the household, and the social responsibilities of domestic intimacy (Y. Castan et al., 1989, p. 136). Privacy came to be understood as the personal privacy of the individual.

It should be pointed out, however, that this perspective does not fit the development of the private sphere of women and certain other groups of people.[61] As women of this period (18th, 19th and a part of the 20th century) were excluded from public office and were confined to the home, it might seem somewhat paradoxical to speak of their private life.[62] Particularly noteworthy for the main topic of this dissertation, is the fact that for those parts of the population that could not (relatively easily) enjoy a private life in the periods before the 20th century, public and semi-public spaces played an important role in achieving privacy. Public spaces were therefore often used for private purposes, particularly by women (for instance, private meetings and discussions were often held during walks). Certainly, there were – and remain – aspects of inequality and instability of the emerging regime of privacy, which depended on gender, race, education, skills of literacy, the comforts of the home, and the threats and opportunities of urban living (Vincent, 2016, p. 50). In fact, in the more distant past privacy was a scarce and contested commodity; it was not a possession or a secure right but an *aspiration* 'whose pursuit required constant vigilance, endless adjustment, frequent defeat and occasional outright conflict' (*ibid*., p. 5). Private life can thus be said to have been more of an exception rather than a rule in general in the past, at least for the majority of the population. Indeed, as Gutwirth (2002, p. 20) notes: 'The historiography of private life has never been easy. The meaning of the term "private" changed from age to age, differed from one social group to another.' However, in the second half of the 20th century, at least in liberal democratic societies, privacy *has* become a standard applicable to most groups in society (although, still, to somewhat various degrees).[63] This development is generally seen as a great achievement.

2.1.3 The many meanings of the term 'private'

This socio-historical development of private life is largely mirrored in the many meanings of the term *private* that the word has come to hold in time (Williams, 1983, p. 242).[64] In this part, I will examine the etymological origins of privacy.

61 See Richardson (2016) and Osucha (2009) on the 'whiteness of privacy' that compare the image of the white woman, who *should* be protected from publicity that demeans, to the image of the black body and the 'racially denigrating visual consumption of African Americans.'

62 Certain feminist legal theorists argue that privacy discourse reinforces a misleading liberal model of society/state relations, concealing gender hierarchies and obscuring social reality that it helps to constitute, instead of opening it up to public scrutiny (MacKinnon, 1987).

63 The mentally ill, the homeless and prisoners, for various reasons, are still granted or achieve a lesser standard of privacy today.

64 Despite the fact that this development of meaning is done for the English word private, a similar development can be said to hold for other languages, where its meaning originates from Latin.

As Williams (*ibid*., p. 242) explains in his succinct account of the historical re-evaluation of the word, *private* came into English (and other globally influential languages, including French) from Latin *privatus*, meaning withdrawn from public life, and *privare*, meaning to bereave or deprive. The earliest meaning of the word when it first came into use in English in the 14th and 15th century therefore represented a certain state of deprivation. Private was applied to withdrawn religious orders (in the sense of seclusion) and to persons not holding public or official position or rank, as in 'a private soldier' or 'private member in Parliament' (*ibid*.). The meaning later acquired the sense of secret and concealment, both in politics as well as in a sexual sense of 'private parts.' According to Williams, there was a crucial moment of transition in the meaning of the word from the 16th century onwards when it started to be used in conventional opposition to *public*, as in 'private house', 'private education', 'private club', and 'private property'. This transition represented a move in meaning from the state of *deprivation* to a state of *privilege*, where the limited access and participation were now seen as an advantage or benefit.

Another notable development began in the 16th century (and developed especially in the 17th and 18th centuries), in which private was beginning to be understood as *independence* and *intimacy*. Seclusion was no longer understood as mere physical withdrawal but as a sense of a quiet life, representing a sense of decent and dignified withdrawal and *the privacy of my family and friends* (Williams, 1983, p. 242). In accordance with this description, Richelet defined the French word *privé* in his *Dictionnaire français* from 1679 as meaning not only 'familiar' but also something like the English expression 'at home', connecting it to space (in the sense of 'he is most *privé* here') as well as to relations ('he is most *privé* with Mr. So-and-so') (as referred to in Chartier, 1989a, p. 400). Already in the 17th century, privacy thus did not require isolation, retreat, or protective walls; rather it was increasingly defined by the ability to choose freely the company with whom one spent time not devoted to routine business and chores. Moreover, the increased availability of books and the progress of literacy in the 17th century, led to the invention of silent reading, which became an intimate activity (Y. Castan et al., 1989, p. 125).

After the 18th century, the 'private' came to be closely related to happiness (at least for the favoured few, protected by law and social institutions), beginning to develop beyond the spatial and familial sense (Hunt & Hall, 1990, p. 9). Williams (1983, p. 242) concludes that the predominant contemporary meaning of the word private that developed in connection to the bourgeois way of life, is that of the realm of the *personal*, representing personal independence as something strongly favourable.

The meaning of privacy, as follows from the etymological origins of the word, can thus be broken down into two main stages. In the first stage privacy represents a state of deprivation, first as physical seclusion and then as its mental counterpart – secrecy. In the second stage, when it is placed in opposition to the public, it begins to represent a state of privilege in a variety of forms: first, in the form of protection offered by the physical home and the family (household) and as protection of the choice and establishment of intimate relations and, finally, of the development and autonomy of the individual.

It should be noted, that the word private today retains the multiple meanings arising from its long tradition (Williams, 1983, p. 242). Private might primarily refer to the individual or personal realm but it also stands in opposition to public life and the state, overlaps with the family and household, represents a state of intimacy, secrecy and seclusion, and has a negative sense as 'private advantage' (or 'private profit', at least from the perspective of critics of capitalism and neoliberalism). The etymological development of the meaning of private hence shows us that the meaning of private, which further affects how we think about privacy, is changing over time so that there is a predominant meaning at a certain time; however, other meanings do not disappear, rather they exist alongside one another. This is connected to our private lives, the ways we live and experience privacy in practice, which have developed in a multifaceted manner so that there is a variety of forms of private life. Or, as Vincent (2016, p. 49) put it, privacy – as a practice and as a term – has an 'evolving character.' This has important consequences for the way privacy is conceptualised in scholarly literature and, perhaps even more so, for the way privacy is implemented as a fundamental human right (see Sections 3 and 4).

2.2 The philosophical foundations of the concept of privacy: a liberal framework

Privacy began to develop as a theoretical concept only in the 19th century with the advent of bourgeois liberalism. The 19th century has thus been called 'the golden age of private life,' the time when the vocabulary and reality of private life really took shape (Perrot, 1990, p. 2). However, the foundations for this 'golden age' were laid in philosophical ideas centuries earlier. It is argued that contemporary privacy theory draws mainly from the thought of three modern liberal political philosophers: Locke, Kant and Mill (Richardson, 2016, p. 4; Rössler, 2005, p. 4). Although these philosophers did not address the topic of privacy directly, their thought strongly influenced privacy scholars in the 20th century and still does today. As the nineteenth-century political and philosophical framework of liberalism forms the foundation of contemporary conceptualisations of privacy (Rössler, 2005, p. 10), one must therefore understand

their philosophical roots in order to understand the role of privacy today (Vogel 2000; in Richardson, 2016, p. 45).

The aim of this Section is not to thoroughly examine the philosophy of Locke, Kant and Mill but to briefly present those aspects of their thought that are relevant for the study of privacy, and to do so in a manner accessible to non-philosophers.

2.2.1 Locke

In his *Essay concerning human understanding* (Locke, 1996 [1689]), Locke put forward a conception of the self that strongly influenced contemporary understandings of privacy. Several key privacy scholars (including Judith Jarvis Thomson and Charles Fried) base their conceptions of privacy on the thought of Locke, particularly his idea of 'property in the person,' according to which humans are owners of their abilities.

Coleman (2005) argues that Locke envisioned a self that, through consciousness and memory of what we have thought and done – a sort of *appropriation*, is able to know that it is a self. A self thus remembers that it thought and acted, so that a 'narrative of life' is produced as a result, for which that individual is responsible. The Lockean self is an isolated individual, which appropriates food and ideas from the outside and then makes them its own. In this sense, the perspective of others is thus missing from this account (Richardson, 2016, p. 97). For Coleman, this idea of a self that is alone in self-definition fits well with Locke's Protestantism and its newly constructed direct relationship between the self and God, moving away from the pre-modern definition of oneself in relation to others or associated with one's status (*ibid*., p. 91). Locke's thought hence emphasizes the inner, what we would today refer to as the 'most private', realm of the person.

According to Richardson (2016, p. 95; cf. Coleman 2005, Balibar 2006), Locke's self thus emerges through consciousness and memory, which are central to one's self-identity. This aspect is particularly important today in light of continuous surveillance and 'big data' analysis techniques (also for the right to be forgotten). Contemporary accounts of memory (Mayer-Schönberger, 2009; Schachter, 2001) see memory as reconstituted each time it is remembered, so that it can be altered and with it our identity and sense of self (of course, depending on the importance we give to the memory). Consequently, the creation of self-identity will be affected by different interpretations of our – and increasingly other's – memory of events. Just like consciousness, which is often described as a 'train of ideas', memory is thus not a stable thing.

Locke's conception of ownership of oneself is, thus, essential for contemporary accounts of privacy that see it as having value for identity building. Furthermore, since privacy and other human attributes can be treated as commodities, Locke's ideas are important in regard to the transition to more neo-liberal perspectives on privacy, which advocate a market approach of commodification of human abilities and attributes that is to be applied to all areas of life; such a neo-liberal subject is governable by being incited to treat herself as an enterprise (Richardson, 2016, pp. 80–81). In Lockean terms, privacy can indeed be understood as a type of property that we own and can alienate through sale or gift. However, the definition of privacy as a type of Lockean property needs to take into account that there is a moral, political and phenomenological difference between 'owning a car' and 'owning a body' (and where 'owning personal information' is closer to the body) (*ibid*., p. 11).

2.2.2 Kant

Alongside Locke, Kant's work on the respect for personhood (or selfhood) had a great influence on modern conceptions of privacy. Among contemporary privacy scholars, Schoeman and Bloustein strongly draw upon Kant's thought (see Section 2.1). Moreover, the Kantian concept of human dignity has been influential in the German (and more broadly European) legal tradition (e.g. Eberle, 1997), particularly as forming the foundation of the right to informational self-determination and the rights of personality (see Section 4).

Kant rejected the idea that any part of a person can be treated as property. His 'categorical imperative' namely demands that one act only in accordance with the maxim through which you can at the same time will that it become a universal law, including the humanity formula of the categorical imperative, according to which humans (rather, our 'humanity') should be treated as ends in themselves and not a means to an end (Johnson & Cureton, 2016; Kant, 2012 [1785]). As such, human beings have 'an intrinsic worth, i.e. *dignity*,' which makes them valuable 'above all price' (Rachels & Rachels, 2015, p. 114; emphasis in original). Furthermore, humans have dignity because they are rational agents – that is, free agents capable of making their own decisions, setting their own goals, and guiding their conduct by reason (*ibid*., p. 115). This is connected to Kant's understanding of personhood, which denotes the ability to use reason in order to think for oneself and is therefore conceptually tied to autonomy and the ability to form a life plan (Richardson, 2016, p. 20).

In the context of privacy, engagement with Kant's idea of personhood is thus tied to the faculty of reason, since to treat others as if they were persons involves treating them as if they were rational, autonomous, free, and of equal moral worth. According

to Kant, one must therefore never manipulate or use people to achieve a certain purpose, no matter how good this purpose might be. This is particularly pertinent in the age of nudging, where human behaviour is increasingly influenced for various benevolent purposes, such as de-escalation of aggression, lowering driving speed and eating healthily (think of the *De-escalate* project; see also Chapter 5).

Kant's understanding of autonomy is based on reason and understood as the ability to make one's own life choices (Richardson, 2016, p. 20). Consequently, since failing to respect privacy amounts to disrespecting a person (that is, failing to treat a person with dignity), violations of privacy are immoral since they breach the categorical imperative. Kant's idea of autonomy is constitutive of duty, since we are autonomous when we obey a law that we give to ourselves (following the categorical imperative). In this way, morality depends on the faculty of reason. Of course, Kant is describing a *hero*, an ideal of a 'fully rational creature'[65] – a person that would behave morally irrespective of the circumstances she would find herself in, a person who would be able to stand up against external (societal or governmental) threat (*ibid*., pp. 56-57). Kant's ideal moral person is thus not influenced by either outside or internal forces (such as self-doubt). Despite the fact that this idea clearly deals with an ideal, it is still a popular image of autonomy, capturing 'a spirit of independence' (*ibid*., p. 57). Kant's hero, thus, does not require a sanctuary from public opinion (as Mill argues; see Section 2.2.3 below) in order to live an unconventional life. However, according to Arendt (1998), he still needs peace away from others (that is, privacy) to think and make moral judgments.

2.2.3 Mill

Mill's philosophical ideas in *On Liberty* (2016, p. 5 [1859]) might already be seen as one of the first conceptions of privacy, understood as 'civil' or 'social liberty' – 'the nature and limits of the power which can be legitimately exercised by society over the individual'. Although his ideas served as the basis for many contemporary conceptualisations of privacy, Mill's thought goes beyond the issue of privacy and does not address it in a direct manner. As such, I will discuss his thought in this Section, as one of the most influential philosophical foundations of contemporary conceptualisations of privacy.

In Mill's philosophy we no longer find the Kantian *hero*, who is able to be morally unaffected by his external surroundings and internal forces. Quite the opposite, Mill was concerned specifically about the possibilities of safeguarding individuality – the

65 A man, rather than a woman, in Kant's opinion (Richardson, 2016). This problematic issue, however, goes beyond the topic of this dissertation.

individual's ability to find happiness – against invasions of a person (one might say privacy), emanating from the state as well as from social pressure. He saw constraints upon individuality and diverse ways of living that result from social manners as even greater than those emanating from the law, and he thought that these constraints have a devastating impact not only for the individual but for also society as a whole. Mill argued that there is no clear answer to the question 'how to live a good life', so that one should not be constantly nudged in (an assumed) *right* direction (Richardson, 2016, p. 28). On the contrary, each person should decide for oneself what is a good life through creative 'experiments in living', providing that one does not hurt others (the 'harm principle'; Feinberg, 1984).[66] However, such experimentation still allows one to learn from others. Mill, thus, advocated a society in which individuals can be eccentric, even self-harming, without interference. A very clear-cut distinction between private freedom and public regulation is thus found in Mill's thought (Rössler, 2005, p. 30). Mill is said to be the first thinker to confront the principles of the complex interrelation of private and public (ibid., p. 215, see ref. 6).

This connects to the idea of autonomy as conceptualised by Mill. According to Mill, liberty allows for an area of 'creative experimentation' free from any urge to self-censor that arises as a result of potential publicity that exposes people to criticism (or worse) from others (Richardson, 2016, p. 53). Accordingly, he referred to autonomy as 'creative individuality'. In his idea of autonomy, Mill differentiated between self-regarding and other-regarding activities – activities that only affect oneself and those that impact upon others. This fundamental division forms the basis for Mill's argument supporting the respect of the individual's right to harm oneself, providing that others are not harmed.

Mill's conception of liberty thus represents a sphere of life, in the sense of self-regarding activities, that is cordoned off against others in order to allow 'experiments in living' (*ibid*., p. 55). 'The only freedom which deserves the name, is that of pursuing our own good in our own way' (Mill 1910, p. 75; as cited in Rössler, 2005, p. 50). Totalitarian societies claim that everything a man is and does has significance for society at large, so that the social significance of our actions and relations overrides any other. Consequently, the public or political universe is all-inclusive: all roles are public, and every function, whether political, economic, or artistic, can be interpreted as involving a public responsibility. On the contrary, the liberal society claims an area of action in which he is not responsible to the state for what he does so long as he respects certain minimal rights of others (Benn, 1984, pp. 239–240). These ideas led to

66 While this position has been disputed in literature (see Jacobson 2000), it remains dominant.

the tradition of liberal individualism, which sees individuals as autonomous islands shielded off from the rest of society (J. E. Cohen, 2013).[67]

Particularly since Mill, privacy began to mean – alongside other meanings – something like 'freedom from interference by the state or society in general' (Rössler, 2005, p. 43). Privacy, therefore, became closely bound up with the concept of (personal) freedom, which constitutes one of the main (if not the main) concepts that the normative meaning of privacy is based on (e.g. J. E. Cohen, 2013).

3. PRIVACY AS A CONCEPT: KEY CONTEMPORARY PERSPECTIVES

The transition from private life as a *mere* phenomenon to privacy as a concept began at the end of the 19th century and gathered full speed in the 20th century, particularly since the 1960s. Despite the many proclamations of deaths, ends and slaughters of privacy that have been made regularly ever since the end of the 1950s (e.g. Froomkin, 2000; Miller, 1971; Packard, 1964; Zelermyer, 1959), scholarly literature and case law on privacy, as well as lay debates on privacy in the media, have not subsided. Quite the opposite, they have expanded so much that privacy-related literature can now be described as a vast ocean that no one can navigate properly. Consequently, privacy theory and the right to privacy have been described as so messy, complex and vast that they have become almost meaningless, some even contemplating the abandonment of the term.[68] Contrary to this prevailing opinion, I posit that privacy – although indeed a multi-faceted concept – is a more coherent notion than is usually claimed (cf. Blok, 2002, p. 277).

In order to uncover the values and aspects of privacy in public and the mechanisms for achieving it, I will first take a wide look at key contemporary privacy theories, structuring them into three levels: the underlying value (or role) of privacy (examining *why* we value privacy), the types of dimensions of privacy (specifying *what* is of value in privacy), and the mechanisms for achieving privacy (showing *how* privacy is achieved). In the first part, where I examine the value of privacy, I give reasons for valuing

67 Although one could also argue that Mill's perspective on liberty is necessary not only for individual happiness but also for society (social good) in general, since it facilitates social progress.

68 E.g. Gloria Gonzalez Fuster at the 2017 Computers, Privacy and Data Protection Conference in Bruxelles; see CPDP 2017: Types of privacy. (2017). Retrieved March 31, 2019, from https://www.youtube.com/watch?v=XvdZ-9eD0tQ.

privacy for the individual as well as for society in general. Consequently, I also address (at least partially) the question of *whom* privacy protects. As the main focus of this dissertation – privacy *in* public space – is connected to a particular place (or places) of privacy protection – a part of the *where* aspect is found throughout the dissertation, most notably in Chapter 7 (conceptualisation of privacy *for* public space). This *de-construction* into the who, what, where, why, and how of privacy will serve as a way of simplifying the intimidating field of privacy theory in order to make better sense of it for the purpose of determining, whether these generally identified values, dimensions and mechanisms of privacy broadly fit, warrant and enable the protection of privacy in public space or whether other conceptualisations should be sought.

3.1 The value of privacy: both individual and social

Broadly speaking, two distinct groups of answers to the questions 'why do we value privacy' and 'why privacy should be protected in society' can be discerned in scholarly literature: those that see the value of privacy in another value (or several other values),[69] and those that claim that we value privacy *in* (intrinsically) and *for* (functionally) itself (Rössler, 2005, pp. 67–71). Hughes (2012, p. 821) further discerns four types of perspectives on the value of privacy: (1) privacy as consisting in a number of interests, which cannot be subsumed into a single concept so that privacy is redundant as a concept; (2) privacy as underpinned by a single value; (3) privacy as underpinned by a cluster of values, which benefit the individual; and (4) privacy underpinned by a cluster of values which benefit the individual, groups and society. Most of the definitions and accounts of privacy in literature are 'functional' (or can at least be interpreted as such), describing privacy as not further reducible in its significance but nonetheless grounded in a norm or value other than itself, for example autonomy, identity development or social relations.

Moreover, scholarly literature on privacy still commonly differentiates between the individual and the social value of privacy in a rather sharp manner (e.g. Hunt, 2011), as if these two sides of the value of privacy are antagonistic or mutually exclusive. The focus on privacy as an individual right and the emphasis on individual control dominated much of liberal legal and philosophical thinking about privacy until the 1990s. Already in the 1960, however, an alternative, although quite complementary, thinking about privacy began to develop but was recognised by legal scholars and philosophers researching privacy to a much lesser degree (Regan, 2015, p. 53).

69 It is possible to further distinguish privacy seen as either serving the purpose of another value or being grounded in another value. Oftentimes, privacy is seen as being grounded in another (more fundamental value or right), which it then also fosters (Rouvroy & Poullet, 2009, p. 59).

Particularly sociologists and other social thinkers, like Merton (1968), Goffman (1959), and Altman (1975) recognised privacy as a social phenomenon and identified it as a component of a well-functioning society. Certain philosophical thinkers in the 1970s, such as Friedrich (1971), Arnold Simmel (1971) and Rachels (1984 [1975]), were also beginning to consider a broader social value of privacy. Nevertheless, their analyses are still based on the functionality and value of privacy in its importance to the individual. While they tried to broaden the interest in privacy beyond classical liberal thought, they did it 'in a way that would both be consistent with liberalism but [would] also expand and revitalize its importance in light of the complexities of modern organizational and technological changes' (Regan, 2015, p. 54).

At the end of the 1980s and particularly in the 1990s, however, privacy scholars began to recognise that a narrow individual rights justification for and basis of privacy was inadequate to the actual importance it played in modern life (*ibid*., p. 54). For example, Simitis posited that privacy should be regarded as a 'constitutive element of a democratic society' (Simitis, 1987, p. 732). The first philosophical scholar to take up the topic of social importance of privacy in a serious and broad scholarly discussion was Schoeman. While in his essential anthology on privacy, Schoeman still largely based the value of privacy in its importance to the individual (Schoeman, 1984, p. 413), in his later book (*Privacy and Social Freedom*), he argues that 'the form and function of privacy [lies] in promoting *social* thinking' (Schoeman, 1992, p. 2). This view was taken up by Regan, who in 1995 argued that privacy is not only of value to the individual but also to society in general – that privacy is a common, a public, and a collective value (1995, 2015).

In the 21st century it seems that the social value of privacy came to the forefront of privacy thought, with influential scholars, particularly in North America, like Solove (2008), Steeves (2009), and Nissenbaum (1997, 2010) who, one way or another, began to emphasise the common good of privacy. In general, they posit that privacy theory by focusing on the common good, can bridge the dichotomous framing of the public debate on security and privacy, and help achieve a more 'common sense' debate on how best to achieve both (Regan, 2015, p. 52). In fact, Regan (ibid., p. 66) agrees that the classical liberal view of privacy is only strengthened when joined by the sociological arguments of Goffman and Altman on the common value of privacy. Moreover, because of the value and role of public space for society (see Chapter 4), arguments in favour of the societal value of privacy have particular worth for privacy in public space. As such, I will emphasise these aspects in particular in the following section.

A perspective connected to the social value of privacy is found in communitarian perspectives on privacy (Etzioni, 1999; Sandel, 1982), although these two, interestingly, do not converse with each other in scholarly literature. Communitarians have criticised the classical liberal perspective on privacy in a similar, though harsher and more divisive, manner than the above theories. They submit that liberal theories conceive privacy as a realm of individual freedom, while forgetting about privacy as the realm of life concerned with specific *practices* also relevant to the community at large (Roessler, 2008).

Communitarian critiques of liberalism argue that constitutional individual privacy rights undermine community values and solidarity, claiming that classical liberal theory wrongly conceptualises the individual as dis-embedded and egocentric. As I will show in the discussion below, it is a misconception to think that a theory of privacy based on the liberal ideas of autonomy and identity-building cannot at the same time conceive the self as relational in nature and contextualised in a number of ways (see also Roessler, 2008).

Following these noteworthy developments in privacy theory, I will not distinguish between the individual and social value of privacy in this dissertation. Instead, I posit that they are two sides of the value of privacy, which are complementary, as the values that serve individuals also serve the society as a whole, and vice versa. In this sense, one could see the individual and the social value of privacy as two sides of a coin. As such, I will discuss both individual and social aspects of the particular concept constituting the value of privacy together.

In this Section, I give a brief account of the most influential answers to *why* privacy should be protected in society. First, I discuss the value of privacy as found in the protection of identity-development. Second, I examine its value in fostering an autonomous life. Third, I discuss grounding privacy in the concept of human dignity. Fourth, I analyse the value of privacy for the constitution and maintenance of intimate and other social relationships. Finally, I examine the value of privacy for democracy and political participation.

3.1.1 Identity-development or personhood

Seeing the value of privacy in its protection of the development of a person's identity or personhood is one of the most common position taken in privacy theory (e.g. Altman, 1975; Hildebrandt, 2006b; Hildebrandt & Koops, 2010; Reiman, 1984).

It is a commonly accepted claim today that the self is a social construction, a situated and embodied being (e.g J. E. Cohen, 2000, p. 1377; Regan, 2015, p. 56; Steeves, 2009, p. 204; C. Taylor, 1997). This means that 'humans are not *born* as individual persons, but *develop into* persons as they relate to their environment and interact with others' (Hildebrandt, 2006b, p. 51; emphasis in original). The main idea here is that the individual only comes to know itself if it becomes an object to itself, thus seeing its own actions from the perspective of the other (Mead, 2015).[70]

This idea is echoed in the thought of the French philosopher Ricoeur (1994), who posits that our sense of self is constructed by looking back upon one's self from a distance – taking the viewpoint of another. In order to achieve this there are two requirements. First, the person must be capable to reflect on herself as if she were another – to take a third-person perspective, anticipating expectations, opinions, profiles or stereotypes of others (what Ricoeur calls *ipse* identity). Such self-evaluation, however, requires a certain level of reflective solitude, a time to 'organize the self' (Park & Burgess, 1921, p. 231), which enables the individual 'to integrate his experiences into a meaningful pattern and to exert his individuality on events' (Westin, 1967, p. 36). Secondly, the self also has to be claimed as being the same over the course of time (what Ricoeur calls *idem* identity) (cf. Marshall, 2008, p. 94). This requires the capability of a certain kind of objectification – a comparison that allows a subject to establish sameness in the sense of similarity or even identicalness. 'The continuity of this relational self implies that the autobiography of the self is continuously re-written in confrontation with the flow of new events that shape one's perception of self, world and others' (Hildebrandt, 2006b, p. 52). In this sense, personal identity is not a static collection of attributes but a dynamic, relational concept (Goffman, 1959).[71]

To be able to act, one thus needs to assess how one's behaviour is understood by others and what meaning they attribute to one's actions, which requires the anticipation of how others anticipate us (Hildebrandt & Koops, 2010, p. 447). Identity construction

70 According to Mead (2015) and also Habermas (1992, p. 176) this can only occur through language that enables each social actor to see her own actions from the perspective of the other, and to see herself as the other sees her – a social object. The process of getting to know ourselves also requires us to play a variety of social roles and seeing them reflected back at us through our social interactions with others. Privacy is thus the result of a process of socialization that is mediated through language (Steeves, 2009, p. 205).

71 People construct their identities through a negotiation of boundaries in which the parties reveal personal information selectively according to a tacit moral code that Goffman (1971, p. 198) calls the 'right and duty of partial display.' More recently, the self has been described as 'flexible, fractured, fragmented, decentred and brittle' (Elliott 2001, p. 2; Marshall 2009, p. 1).

therefore takes place in the midst of this anticipation, either rejecting the way we think others are assessing (profiling) us or embracing (including shades in between) the way we are being 'identified'. By either accepting or rejecting the third person perspectives that we think others to have formed of us, we engage in a process of continuous (mostly intuitive) self-construction or identity building.

Moreover, privacy enables us to present to others only those parts of our selves that we want them to see, and which enables us to put forth different versions of our selves in different contexts. According to Goffman (1971, p. 270), life is a dramatically enacted thing, in which we paint a portrait of ourselves, accentuating certain matters and concealing others. The self is thus a 'performed character' (Goffman, 1959, pp. 252–253). Indeed, we show ourselves differently to our children than we do to our colleagues, to our bosses and employers or to our intimate friends. This is connected to the enhanced need of the individual to sustain an acceptable image of herself, since – as I've discussed above – an individual is for herself to a large extent what others have come to see her as. Consequently, this 'enactment' does not only or primarily refer to 'putting up appearances',[72] rather it serves the purpose of self-*production*, as a part of our anticipation, rejection or acceptance of others' assessments of us. The process of coming to know ourselves, namely, requires us to play a variety of social roles (Mead, 2015). In the process of trying on different roles and seeing them reflected back at us through our social interactions with others, we come to know who we are. As Park put it:

> 'It is probably no mere historical accident that the word person, in its first meaning, is a mask. It is rather a recognition of the fact that everyone is always and everywhere, more or less consciously, playing a role … It is in these roles that we know each other; it is in these roles that we know ourselves' (Park 1950, p. 249; as quoted in Goffman, 1959, p. 19).

72 As Goffman (Goffman, 1959, p. 70) pointed out over half a century ago, there seems to be in Western culture a common-sense distinction between the real or sincere performance and the false one, which the fabricator assembles for us. We tend to see 'real' performances as something not purposely put together, an unintentional product of the individual's unselfconscious response to the facts in the situation. The contrived *performance* is thus a painstaking pastiche of false items, representing no reality to which the items of behaviour could be a direct response. 'The legitimate performances of everyday life are not "acted" or 'put on' in the sense that the performer knows in advance just what he is going to do, and does this solely because of the effect it is likely to have' (*ibid*., p. 73). In fact, the ordinary individual is often incapable of formulating in advance the movements of her eyes and body or the content of her statements.

When a performance is given, however, it is usually given in a highly bounded region and limited in respect of time. In fact, the performance that is given highly depends on the context in which it is given. In sociological research, this has been called audience segregation, which is a device not only for fostering impressions but, as explained above, a part of our identity production. The incapacity to maintain this control leaves the performer in a position of not knowing what character she will have to project from one moment to the next, making it difficult for her to effect a 'dramaturgical success' in any one of them. Hence, when audience segregation fails and an outsider happens upon a performance that was not meant for him, difficult problems in impression management arise. When this lack of control is experienced too often, however, bigger issues related to our identity production and management arise.

Privacy is thus important because it allows us to construct borders between the different roles that we play and to keep things off-stage while being on stage in a certain role. In this sense, privacy has been defined as 'the process of boundary negotiations that allows a person *to hold together while changing*; it presumes some measure of autonomy, some real contact like intimacy and some space to rebuild the self in accordance with one's past while anticipating one's future' (Hildebrandt, 2006b, pp. 51–52; emphasis in original).

3.1.2 Autonomy

Closely associated (and partially overlapping) with the value of privacy in relation to identity development, is the position, which sees the value of privacy in fostering and sometimes as a precondition for an autonomous life. Personal identity is thus intricately connected to autonomy, but their precise relationship goes beyond the purpose of this Chapter. It will suffice to state that one's capacity for autonomy may be considered a part of one's identity, which may or may not come to fruition or be developed (Marshall, 2008, p. 90).

The concept of autonomy within the liberal tradition does not have one single unitary meaning. It has its roots in the Millian idea that provided others are not harmed, each individual should be entitled to follow their own life plan in the light of their beliefs and convictions (Marshall, 2008, p. 57; referring to Kymlicka 1989 pp. 9-19). In this sub-section, I will follow one of the most philosophically developed accounts of autonomy in privacy theory, that of Rössler (2005), complementing it with additional insights from autonomy scholarship.

Following Kant and Mill, Rössler bases her conceptualisation of privacy on autonomy, which she understands as a certain kind of freedom. She defines privacy as control over access by others and thus as protection against unwanted access from other people, defined both as actual physical access (to spaces) and as metaphorical access to one's personhood (in the sense of access to information as well as possibilities for intrusion and intervention in a person's behaviour) (*ibid*., p. 43). Rössler submits that we value and indeed should value privacy for the sake of our autonomy, since in a liberal society privacy has the function of permitting and protecting an autonomous life and only a life lived autonomously can be a rewarding life (*ibid*., p. 1).

One of the defining characteristics of liberal societies is the idea of individual freedom. Such a society wants to provide their citizens with possibilities for living their life in accordance with their own particular ideas about what makes a good life. Rössler is referring to a specific kind of freedom – freedom as autonomy, since one must be free to be autonomous, but not every free action is an autonomous one (2005, p. 49). It is of no surprise then that autonomy has been called the 'close cousin' (Carter, Kremer, & Steiner, 2007, p. 323) and the 'twin' (Christman, 2014) of positive freedom. This sort of freedom implies not only certain conditions of autonomous action but also a certain practical relationship to one's own actions and hence to one's own selfhood (Rössler, 2005, p. 43). For Rössler, a person is autonomous not only if she can ask herself the question what sort of person does she want to be and how does she want to live, but also if she can then actually live in this way (at least to a certain extent) (*ibid*., p. 17). Personal autonomy is thus a gradual concept (as one is always more or less autonomous), dependent on subjective abilities as well as external conditions that are necessary for its effectiveness.

According to Rössler (*ibid*., p. 50), a life lived autonomously is first of all one for which we can give ourselves (good) reasons. It requires reflection, asking oneself certain questions: how do I want to live, what kind of person do I want to be, and how should I best strive for my own good in my own way (*ibid*., p. 51; referring to Tugendhat). Rössler thus defines *personal autonomy* as self-determination, describing it as a certain relationship of the person to what she chooses (the object of choice) and how she chooses it (the mode of choice) (2005, p. 51). As such, this self-determination requires constant updating (similarly Dworkin, 2014, p. 61).

But how does this *personal good* relate to the social good or morality more generally? In this respect, we can distinguish between 'moral' and 'personal' autonomy. Moral autonomy refers to the capacity to subject oneself to objective moral principles (following Kant). In this sense, a person is capable of rational choice through exercising

her own moral judgements governed by moral law (Dworkin, 2014; Marshall, 2008, p. 58). Personal autonomy, on the contrary, is an (allegedly) morally neutral trait that individuals can exhibit relative to any aspects of their lives not limited to questions of moral obligations. As Waldron (2005, p. 307; as cited in Marshall, 2008, p. 58) put it: '[t]alk of personal autonomy evokes the image of a person in charge of his life, not just following his desires but choosing which of his desires to follow. It is not an immoral idea, but it has relatively little to do with morality.'[73]

Nevertheless, individuals' exercises of their personal autonomy should be (at least to a certain extent) amenable to the demands of shared moral norms (Marshall, 2008, pp. 58, 64). This is connected to the fact that autonomy – counter to the common liberal depiction of the concept – does not exist on its own, independent of context in which the individuals who exercise it are living. Autonomy is, namely, often presented as a quality of an independent, isolated, 'atomistic' and 'unencumbered' individual (*ibid.*, p. 62). Yet, individual autonomy and the interdependence of persons are not binary opposites. In fact, many classical liberal philosophers (including Raz, Kymlicka, Rawls and Dworkin) acknowledge the role that social embeddedness (representing a complex matrix of social, economic and psychological factors, which affect the possibility of developing into an autonomous being) plays in relation to our concept of ourselves and making our own decisions in life (E. Jackson, 2001). Many recent theorisations of autonomy thus try to reconceive autonomy, aiming to retain the indispensable notion that people should be free to make their own choices (self-determination), while acknowledging the socially constructed quality of the choices people make (e.g. Jackson, 2001).[74] Taylor (1997) thus argues that self-determination must be conducted against an existing set of rules or a gridwork of moral measurement. As Marshall (2008, p. 59; emphasis in original) put it:

> 'Autonomy is therefore seen as a *capacity* that has to be developed – it can flourish through human relationships or lie undeveloped [Nedelsky 1989]. It is therefore not concerned with isolation but depends upon the existence of relationships that provide support and guidance: relatedness is not the antithesis of autonomy but its precondition.'

73 This is connected to the distinction between 'moral' and 'personal' autonomy. Moral autonomy refers to the capacity to subject oneself to objective moral principles (following Kant). In this sense, a person is capable of rational choice through exercising her own moral judgements governed by moral law (Dworkin, 2014). Personal autonomy, in contrast, is an allegedly morally neutral trait that individuals can exhibit relative to any aspects of their lives not limited to questions of moral obligations.

74 Rössler acknowledges this point but develops it to a lesser degree.

In this sense, we can say that 'a concern for autonomy is a concern to enable people to have a good life in a social setting' (ibid., p. 64). Similarly, Cohen identifies a 'dynamic theory of individual autonomy', where the individual is valued as an agent of self-determination as well as community-building (J. E. Cohen, 2000, p. 1377).

Finally, according to Rössler autonomy requires privacy (they thus have a functional connection) because we learn to develop autonomy as part of our *habitus* – it is only through the (symbolic) *spaces* delineated by the borderline between private and public that the development and exercise of autonomy becomes possible (2005, pp. 60, 73). Consequently, an autonomous life is only possible in conditions where privacy is protected.

3.1.3 Human dignity

Closely connected to the concept of autonomy (and consequently to identity) is the concept of human dignity (sometimes called personal inviolability). Human dignity is often described – with good reason – as an 'especially vague and ambiguous concept' (Jackson, 2016, p. 26). The main issue of basing privacy on human dignity, even more so than in regard to identity and autonomy, is that it remains very much obscure (and questionable) which interpretation of human dignity may provide a solid foundation for privacy (Floridi, 2016, p. 308). It thus runs the risk of explaining *ignotum per ignotius* – what is unknown (privacy) by what is even more unknown (human dignity), to use Galilei's phrase (*ibid*.). As such, it is not the most commonly used approach to ground the value of privacy nowadays. As I clearly do not attempt to resolve these philosophical matters here, I will merely follow one of the most influential theories of privacy based on human dignity, supplementing it with additional insights.

Benn's conceptualisation of privacy based on personal inviolability rests on the principle of respect for persons as choosers (1984). Benn understands a person as 'a subject with a consciousness of himself as agent, one who is capable of having projects, and assessing his achievements in relation to them' (*ibid*., pp. 228-229). In order for someone to be a person, she thus needs to be autonomous and understand that her life is a kind of 'enterprise of one's own.' Benn (similarly to Kant) thus connects respect for human dignity to the promotion of autonomy. Similarly, Raz (1979, p. 221; as quoted in Marshall, 2008, p. 23) states that 'respecting human dignity entails treating humans as persons capable of planning and plotting their future.

Thus, respecting people's dignity includes respecting their autonomy …'.[75] According to this perspective, human dignity works in an empowering manner, as it protects the capacity of the individual to make unforced choices (be personally autonomous), thus equating human dignity with autonomy.

According to Benn (who follows Sartre's notion of 'scrutiny of the other'), to observe someone is 'to take away liberties,' to show less than a proper regard for human dignity (1984, p. 227). Covert observation or unwanted overt observation thus deny respect for a person because they transform the actual conditions in which the person chooses and acts, thus making it impossible for her to act in the way she set out to act, or to choose in the way she thinks she is choosing. For what others know about the person can radically affect her view of herself. Moreover, to treat the collection of personal information about her as if it raised purely technical problems of safeguards against abuse it is to disregard her claim to consideration and respect as a person. According to Benn, the focus on informational privacy is thus unjustified, as privacy covers particularly one's body and those things, which the conventions of a culture may cause one to think of as part of one's identity (e.g. one's possessions and thoughts).

However, equating human dignity with autonomy is problematic. According to Beyleveld and Brownsword (2001; cf. Jackson 2006), in recent years the meaning of the concept of human dignity has shifted. 'Human dignity as empowerment' has supposedly become 'human dignity as constraint', as the concept is being increasingly invoked in order to restrict individual's choices by, for instance, arguing that some types of action are 'against human nature'. In the 'human dignity as constraint' regime, autonomous action is limited by reference to the duty not to compromise one's own dignity (Marshall, 2008, p. 27). Writing about human dignity as a legal value, Feldman (2002) similarly posits that recourse to human dignity on the side of the state means that the state may introduce regulations to restrict the freedom and choices people can make, when it takes a particular view on what is required for people to live dignified lives. Human dignity used as a legal tool is thus a two-edged sword.

Taking into account the discussion on autonomy above, we can see that the concept of human dignity, at least as connected to privacy, is intricately connected to the moral

75 Similarly, Floridi (2016, p. 310) claims that human dignity rests in our ability to be the masters of our journeys and to keep our identities and our choices open. Human dignity has also been said to be violated in cases, when people are treated as objects even in the pursuit of benevolent goals, if the decision-making is taken over by others against a person's will (Pedain, 2003).

type of autonomy (rather than personal autonomy). This means that the concept of human dignity as a basis of privacy *can* bolster individual freedom *if* one chooses to make choices that the community perceives as a dignified or 'good' way to live (Marshall, 2008, p. 29). There is thus a risk that human dignity can force certain conceptions of the 'good life' on people. At least from a libertarian perspective, one might thus conclude that it might be better to search for the value of privacy in the concept of (personal) autonomy itself, which gives the possibility of a broader range of actions in order to choose one's own way of life.

3.1.4 Intimate and other social relationships

Another common way of identifying the value of privacy is seeing privacy as making intimate or sometimes broader social relationships possible (e.g. DeCew, 1997; Fried, 1984; Hughes, 2012; Roessler & Mokrosinska, 2013; Steeves, 2009; Thomson, 1975). Forming relations with others – creating one's social identity – is an important part of building one's identity or, rather, identities (Jenkins, 2014). In this sense, there is a significant connection between this and previously discussed underlying values of privacy. However, the focus on the possibility to forming and maintaining social relations puts more emphasis on the value privacy has for society more broadly, showing that privacy is inherently social, since it is a part of the way in which social beings interact (Steeves, 2009, p. 196).

Intimacy can refer to various states of our private life. Sometimes 'intimate' is used to describe seclusion and solitude, more often, however, it denotes certain close relationships (e.g J. L. Cohen, 2004; DeCew, 2018; Gerety, 1977; Gerstein, 1978; Inness, 1992). Westin's concept of the intimate zone (or sphere), for example, goes beyond intimate sexual relationships and refers to a state where the individual is acting as part of a small unit, including relationships with family, friends, and work colleagues. The intimate sphere can, however, be defined more or less broadly (see e.g. Koops et al., 2017). Despite the fact that the boundary between the intimate and non-intimate sphere cannot be pinpointed, the value of understanding privacy as making intimacy possible lies elsewhere – it lies in providing the indispensable setting for certain types of relations (however narrowly or broadly one might define them for oneself) and the development of an articulate inner life.

Many authors see a strong connection between privacy and intimacy, some positing that intimacy could not even exist without privacy (e.g. J. L. Cohen, 2004; Gerety, 1977; Gerstein, 1978; Inness, 1992). Gerstein (1978), for example, defines intimacy as an experience of a relationship in which we are deeply engrossed and, which we cannot continue to be immersed in, if we begin to observe ourselves or other things around

us. Intimacy is thus characterised not only by its intensity, but also by the significance it has for those caught up in it. This is connected to the important difference between the way we experience our actions when we intend them to be observed and understood by others and the way we relate to them when we are immersed in intimacy. According to Gerstein (and in line with the view of existentialist philosophy, particularly of Sartre), when we intend our actions to be observed, our sense of them is similar to that of the observers: 'we watch ourselves to see what sort of a point our actions appear to be making, just as they watch us in order to get the point' (*ibid*., p. 78). This means that the person does not experience the relationship from within, rather, she is an observer of herself. Intimate relationships are thus characterised by a particularly vulnerable, fragile sort of interpersonal communication, which falls apart or becomes seriously distorted if the principles of publicity (open access, inclusion, availability of information) are applied to them (J. L. Cohen, 1997, p. 143).[76] Intimacy therefore desperately relies on privacy as a special boundary in regard to the outside.

Furthermore, this account of privacy also has a broader role in protecting our freedom, since it allows us to do or say things, which are not forbidden by morality or law but are nevertheless unpopular or unconventional. In this sense, intimacy assists us in developing an articulate inner life, by permitting us to explore non-public feelings in something other than solitude and to learn about the comparable feelings of one's intimates (Nagel, 1998, p. 18). Persons, namely, often share thoughts and opinions with those closest to them, which might not fare too well with the general public, such as things that are considered taboo or politically incorrect. While this might sound undesirable (e.g. expressing racist opinions), political theorists argue that such a 'ventilation system' (of frustrations) might nevertheless serve a greater societal goal, by preventing greater harms (e.g. physical attacks on particular persons one might not like) (e.g. Mouffe, 2013; Sennett, 1992b).

This, however, does not mean that we fully and indiscriminately share our inner life even with our partners and closest friends. Restraints of privacy apply to even the closest relationships and to be deprived of this control, according to Fried (1984), would be an assault on liberty, personality, and self-respect. Humans are highly complex and diverse beings, so that the full range of what they feel, want and think would not fit into a common space without generating uncontrollable conflict and offense. As

76 Similarly Fried (1984, p. 205) posits that privacy is not just one possible means among others to insure some other value, but that it is 'necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust."' These fundamental relations require the possibility of privacy for their existence.

Nagel (1998, p. 28) put it: 'The distinction between what an individual exposes to public view and what he conceals or exposes only to intimates is essential to permit creatures as complex as ourselves to interact without constant social breakdown.'[77]

Finding the value of privacy more broadly in developing non-intimate social relationships, is also a noteworthy perspective in privacy theory, stemming particularly from sociological research (e.g. Altman, 1975; Merton, 1968; G. Simmel, 1964). We namely build our social identities not only (or even primarily) by developing the closest ties with others (e.g. between family, lovers and close friends, which involve the sharing of personal, biographical, idiosyncratic and often emotional aspects of the self; called 'primary relationships' in sociology) but by forming looser ties with those alike and those different, in which only very limited categories of the self are brought into the interaction (called 'secondary relationships'; Lofland, 1998, p. 54). This includes social interaction with a wide range of actors, including acquaintances, work colleagues, strangers, professional relationships (e.g. interacting with a doctor), and other secondary types of relationships.

In all of these relations we play a certain role (or roles), revealing only certain parts of our lives, although to varying degrees (and to varying success). For example, in the workplace one plays the role of the employee or co-worker, in the park the role of a dog-owner, a beer-connoisseur in the pub or a concerned inhabitant on the streets of Rotterdam. The reason why we can play these distinct social roles in different contexts – even when these occur in (semi)public spaces, therefore, in principle, observable to an unrestricted group of others – is partly because of social norms that govern them and partly because of the spatial constraints that keep them distinct.[78] As Goold (2009, p. 4) put it:

> 'Without privacy, it not only becomes harder to form … [intimate] social relationships – relationships based on exclusivity, intimacy, and the sharing of personal information – but also to maintain a variety of social roles and identities.'

77 Similarly put by Simmel (1964, pp. 311–312): 'All we communicate to another individual by means of words or perhaps in another fashion – even the most subjective, impulsive, intimate matters – is a selection from that psychological-real whole whose absolutely exact report (absolutely exact in terms of content and sequence) would drive everybody to the insane asylum.'

78 For more on this see Nissenbaums (2010). Nissenbaum posits that privacy is about 'context-relative informational norms' (*ibid*., p. 129) that 'govern the flow of personal information in distinct social contexts (e.g., education, health care, and politics)' (p. 3). In other words, privacy is about what is appropriate for different groups to know about us given the nature of the information and the context in which it is shared.

In this sense, privacy is constitutive of social relationships – it is a necessary (although not sufficient) condition of social relations. In other words, it is not only that privacy makes social life *bearable* (Oravec, 2003, p. 9) it is also that privacy makes social life *possible*. 'The formation and maintenance of social relationships depends on discretion, concealment, and retreat as much as on openness, revelation, and coming together' (Kasper, 2007, p. 175).

These social norms are, of course, broken all the time, at least to a certain extent. Sometimes this leads to a minor annoyance, such as when fellow yogis at your yoga studio ask you about your income. On other occasions, they can lead to defective social relations with more serious consequences. For instance, failure to meet expectations of workplace privacy has been shown to lead to uncertainty on the part of the employees, a considerable deterioration of the atmosphere at work and a general deterioration in employee motivation – ultimately, to 'dysfunctional role behaviour' (Roessler & Mokrosinska, 2013, p. 780). However, social relations can become defective not only when privacy norms are broken by the participant of the social relationship itself, privacy norms regulating the relationship can be violated from the outside, 'causing failure in adherence to those norms through invasion of the privacy of the relationship' (ibid., p. 780; Korsgaard, 2009). This is precisely what happens when persons are surveilled in their various roles through technology, such as wifi tracking and sound sensors in public space, especially when these parts of our life are then connected, potentially leading to negative consequence in other parts of our lives, as well as revealing an ever fuller and clearer picture of our lives.

According to Roessler and Mokrosinska (2013, p. 775), in light of this external threat to our associational privacy, we need not only 'privacy (of individuals) *within* the relationship' (participants of the relationship adhering to the privacy norms) but also – and increasingly so – 'privacy *of* the relationship'. In other words, we need a level of privacy in the forming and enactment of the relationship itself, since the function and intention of these relationships can be realised only if their privacy is protected. In this sense, the interest broadens from a *mere* individual interest in protecting privacy *in* relationships to a broader societal interest in protecting the privacy *of* relationships. Social relationships, particularly those among strangers, are not only morally valuable for the individuals involved but also directly serve to promote social integration (*ibid*., p. 776) and social solidarity (Kasper, 2007), which they do *through* as well as *by facilitating* general social trust. A nice exchange with a stranger on the street is namely only possible when a certain level of general social trust already exists; but such an exchange also facilitates the development of more social trust (this will be developed further in connection to privacy in public space, particularly in Chapter 7).

3.1.5 Democracy, participation and political autonomy

It has already been established in the above sub-sections that privacy not only has value for the individual (in order to develop her autonomy, identity and social relationships) but is also an essential component of a (well-)functioning society. In all of the above accounts, privacy has value for individuals as individuals and/or to all individuals in common. However, according to some privacy scholars, privacy also has value first and foremost for society – more precisely, a democratic liberal society.

Regan (1995, p. 50) has argued than privacy is not only a *common* value in that all individuals appreciate some degree of privacy and have some shared perceptions about privacy,[79] it is also a *public* value in that it has worth (broadly) to all aspects of the democratic political process.[80] The connection between democracy and privacy is neither very new nor is it rare. Already in 1980, Gavison (1980) posited that privacy contributes to the protection of liberal, democratic and pluralistic societies. Similarly, Simitis (1987, p. 732) posited that privacy should be regarded as a 'constitutive element of a democratic society'. Later, authors have claimed that, on the one hand, privacy is a precondition for constitutional democracy, including for the exercise and fulfilment of other values and rights in a democratic society (Boehme-Neßler, 2016; Hildebrandt & Koops, 2010, p. 446). In this sense, privacy can be seen as having either a functional or an essential value for democracy. I agree with Lever (2015), however, that there is no particular need to sharply distinguish between instrumental and intrinsic justifications of privacy, as the former can be as important for our freedom and equality as the latter, so I will not pursue this distinction any further here. Some have even claimed that a theory of privacy cannot ultimately be elaborated without a theory of democracy (Roessler, 2008). There is thus a strong and bidirectional relationship between privacy and democracy. I will not delve too much into the difficult and problematic concept of democracy here, as that is not the focus of this dissertation. I will rather focus on the connection between privacy and the main ideas that underpin and justify democratic government and democracy as a key political concept today.[81]

79 Supported by public opinion data from the 1970s to the 1990s (Regan, 1995, pp. 50–68). Similarly as with the freedom of conscience, individuals may believe in different religions or none at all, but they similarly acknowledge the importance of freedom of conscience.

80 According to Regan (1995, 2015) privacy is also a *collective* value, since technology and market forces are making it difficult for any one person to have privacy without all other persons to have a similar minimum level of privacy. See also Mantelero (2017) on the idea of collective privacy.

81 In practice, of course, democracies can take a variety of different forms and we can think of them in more idealistic or realistic terms and the familiar gaps between them. I will not be concerned with (the necessarily imperfect) democracy in practice here, instead I will focus on the conceptual underpinnings of the key political idea.

Democracy is essentially a distinctive way of organising social life. The most basic idea underpinning democratic government is that its governments are elected by universal suffrage, and where people have an equally weighted vote and are entitled to participate in collective decisions, no matter their wealth, knowledge, virtue, or pedigree (Lever, 2015, p. 166).[82] Democracies thus entitle people to form a variety of associations (including political parties and interests groups but also scientific societies, families, hockey-clubs, and other associations of the like-minded) through which to advance their interests, express their ideas and beliefs, and fulfil their duties as they see them (*ibid*.). However, in order for individuals to participate in these ways in a democratic government, they must first become citizens – not only in the sense of being recognised as citizens by the state but developing democratic awareness and capability. The foundational relationship between privacy and democracy is, thus, based on the democratic requirement of and social interest in developing autonomous citizens with democratic awareness (Boehme-Neßler, 2016, p. 227). According to Brettschneider (2007, p. 76), privacy is intrinsically valuable in a democratic society because of its link to autonomy – no longer personal but rather political autonomy (*ibid*., p. 3).[83] Although we are inherently intersubjective beings, we are not first and foremost 'public' beings, in other words, citizens (Dewey, 2016; Jacobson, 2010). To become a citizen, that is to act as an independent and self-controlled agent, that has developed the behaviours and attitudes necessary for citizenship, and to do so in a shared space in the public arena (that is in public space), is something that we can successfully do only by emerging from our private and familiar territories, most notably, our homes.

Political autonomy is thus an essential value for any substantive (as opposed to purely procedural) conception of democracy. According to Brettschneider (2007, p. 3), political autonomy is one of the core values of democracy (including equality of interests and reciprocity), protecting the rights of citizens as (as free, equal and reasonable) political participants and guarantees them certain substantive protections from state coercion,

82 The Stanford encyclopedia of philosophy defines democracy as 'a method of group decision making characterized by a kind of equality among the participants at an essential stage of the collective decision making'; see Christiano, T. (2006). Democracy (Stanford Encyclopedia of Philosophy. Retrieved March 25, 2019, from https://plato.stanford.edu/entries/democracy/.

83 It is intrinsically rather than functionally valuable because of Brettschneider's value theory of democracy and its relationship to his critique of a purely proceduralist understanding of democracy, according to which a democratically elected government is the way to make, justify and execute collectively binding decisions. As Joshua Cohen (Pluralism and proceduralism, 1994) has shown, while democratic government indeed has an important procedural element, the pure proceduralist is wrong to think that we can identify a set of democratic procedures without appealing to assumptions about what is valuable, desirable, useful and right (Lever 2015, 168).

especially in relation to public space. Privacy as a *public* value thus also refers to privacy as a means of establishing boundaries on the government for the exercise of power in the public realm of life. Moreover, there is a pressing need of the limitation of use of power of corporations and other private actors, which increasingly take on public tasks (and thus power), particularly on the level of municipalities (as discussed in Chapters 1 and 4). This is important in relation to the protection of explicit civic (political) life, including public protests and the secret ballot. In this sense, this aspect of the value of privacy goes beyond the value of privacy in relation to personal autonomy.

According to Brettschneider (2007, p. 75), the secrecy of voting illustrates the importance of privacy to democratic politics, since, in deciding how to vote, citizens are entitled to freedom from coercion through a 'private space' (the booth), in which to make up their own minds and exercise political judgment. Moreover, the privacy of the voting booth serves to enhance our sense that we are free to make and enact our own decisions without external coercion and the more general role of privacy rights in the citizen's capacity to think of themselves as *rulers*. Our capacity for political thought is, namely, intertwined with our capacity for thought in general, so that a society which is concerned with respect for these capacities needs to value the citizens' ability to be free from coercion.

Connected to the role of privacy in public for democracy in general, is its role in the forming of multiple publics, in other words, public spheres (Regan, 2015, p. 61; see also Chapter 3). In order for the democratic *competition* of ideas to work, there is, namely, a need for several different competing ideas and opinions (Boehme-Neßler, 2016, p. 227). Deviating opinions and unusual ideas that are necessary for a vibrant democratic discourse, naturally require free and mature citizens who can form independent opinions and stand up for them. Only such discourse makes the competition of ideas possible, moreover, only in this way can the decision of the majority be democratically legitimised.

Similarly, Arendt (1958, p. 38; as quoted in Regan, 1995) posits that in order for the 'common' to develop in the public realm (creating a 'community of one's peers'), there must be the 'simultaneous presence of innumerable perspectives and aspects in which the common world presents itself and for which no common measurement and denominator can ever be devised'. Regan (2015, pp. 61–62) finds telling evidence for this part of the value of privacy in the way candidates, political parties and interest groups are collecting, analysing and using personal information to foster polarization and partisanship in contemporary electorate, as we have recently witnessed particularly in the U.S. with the 2016 elections and the UK 'Brexit' campaign (see

Borgesius et al., 2018; similarly Solove, 2002).[84] This illustrates in a very telling way what such segmentation and targeting messaging means for democracy in general and the publics specifically.

3.2 Dimensions and types of privacy

While some theories of privacy develop essentialist or unitary conceptions of privacy with a unified conceptual core ('a common set of necessary and sufficient elements that single out privacy as unique from other conceptions'; Solove, 2002, p. 14), others offer typological or pluralist conceptions by making meaningful distinctions between different types of privacy (e.g. Koops et al., 2017). The latter type is a mainly descriptive method of conceptualisation (often based on what particular legal systems actually protect) that maps out, that is classifies, types of privacy in a more or less systematic manner. It thus asks the question, *what* does privacy protect. According to this approach, privacy – a complicated concept that cannot be boiled down to a single essence – can be captured by a set of related concepts that together constitute privacy (Koops et al., 2017, p. 488). As such, this type of conceptualisation mainly serves as an analytic tool that can assist in structuring and clarifying the normative privacy debate. In this Section, I will present two notable attempts to classify privacy: first, Westin's four privacy states, which have been highly influential in literature, and, second, a recent systematic attempt to identify the various types of privacy by Koops et al.[85]

3.2.1 Westin's four privacy states

In the 1960s, Westin drew from Prosser's (1960) now famous classification of civil privacy violations ('torts' in common-law language) recognized by US courts[86] and developed a broad theory of privacy, including a description of four states of privacy. Westin's influential book (1967) also explored privacy's psychological, sociological, and political dimensions based on leading theoretical and empirical studies of the

84 Also see: Cadwalladr, C. (2017, May 7). The great British Brexit robbery: how our democracy was hijacked. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

85 As Solove's classification of privacy *harms* (A taxonomy of privacy; 2006) is not a typology of privacy *per se*, rather it is a taxonomy focused on harms and not on types of privacy as such, it will not be discussed here. For descriptions of other typologies (Clarke 1992; Allen 2011; and Finn et al. 2013), see Koops et al. (2017).

86 Prosser (1960, p. 386) identified and proposed four categories of privacy torts from U.S. case law on the matter of privacy at the time: '1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness'.

time (e.g. Ardrey, 2014 [1966]; Hall, 1990 [1966]). Based on this research he defined four basic states of privacy, focusing on the individual and individual experience in daily life, while nevertheless recognising the social nature of privacy. These states are, in increasing level of the individual's involvement with the public sphere: solitude, intimacy, anonymity and reserve.

The first and ultimate state of privacy, according to Westin (1967, p. 31), is solitude. Solitude exists when an individual is separated from others – regardless of other physical, sensory stimuli, or 'psychological intrusions' such as the belief that he is watched by a God or some supernatural force, or even a secret authority. Solitude also subjects a person to the inner dialogue with mind and conscience so that its function is the development of personal autonomy. According to Westin (*ibid*., p. 31), solitude is 'the most complete state of privacy an individual can achieve.'

Intimacy, the second state of privacy, refers to a state where the individual is acting as part of a small unit, allowed seclusion to achieve a close, relaxed, and frank relationship between one or more additional individuals. Westin's definition of intimacy is broader than the everyday meaning of the word, referring not only to the intimate relations between lovers or spouses, but also to family, friends, and work colleagues. He emphasizes that the result of close contact, either relaxed or hostile, is not definitive of the state – instead, the state of intimacy is the prerequisite for that close contact, whatever its results may be.

Anonymity is the third state of privacy, where the individual is in public space but still seeks and finds freedom from identification and surveillance. Anonymity is an essential part of Simmel's (1964) 'phenomenon of the stranger' (Steeves, 2009, p. 197).[87] Anonymity branches out into two sub-categories, or 'sub-states'. The first occurs when an individual is in public spaces with the knowledge that others may observe him or her. However, the person does not necessarily expect to be personally identifiable and thus held to the full rules of expected social behaviour by those observing. As such, anonymity is constructed socially through recognition by others that the anonymous person should not be 'held to the full rules of behaviour that would operate if he were known to those observing him' (Westin, 1967, p. 31). The second kind of anonymity state can be found in anonymous publication: communicating an idea without being

87 Westin used Simmel's insight that strangers 'often received the most surprising openness – confidences which sometimes have the character of a confessional and which would be carefully withheld from a more closely related person' (Simmel 1950, p. 408; as cited in Steeves, 2009, p. 197).

readily identifiable as the author, especially by state authorities. Westin notes that both states of anonymity are characterized by the desire of the individual for 'public privacy' (*ibid*., p. 32).

The final state of privacy is reserve. Reserve involves what Westin calls the creation of a 'psychological barrier against unwanted intrusions' that is exhibited during social interaction, when the need to limit communication about oneself is protected by the willing discretion of those surrounding him or her (Koops et al., 2017, p. 497). It is rooted in Simmel's concept of 'mental distance'. This state is based on the need to hold some aspects of our selves back from others, either as too personal and sacred or as too shameful and profane to express. Reserve expresses the individual's choice to withhold or disclose information; as such it is a 'dynamic aspect of privacy in daily interpersonal relations' (Westin, 1967, p. 32).

Westin's categorization of privacy differs from Prosser's (and Warren and Brandeis's) purely harm-based legal interpretation, turning to privacy *types* (Koops et al., 2017, p. 497). Westin links privacy directly to the needs of individuals, and his classification captures key elements of what privacy is by relating it to specific values that can help to explain privacy and to examples of situations in which privacy is threatened.

3.2.2 The privacy typology of Koops et al.[88]

The most recent and arguably most extensive attempt at a typological classification of privacy was done by Koops et al. in 2017. This attempt aims at systematic and comprehensive classification of privacy, which can serve as an analytic and evaluative tool to help assess the impact of new technologies, social practices, and legal measures on privacy interests that go beyond informational privacy and data protection (Koops et al., 2017, pp. 487–488). This typology attempts to identify types of privacy through an analysis of constitutional protection of privacy (including European Court of Human Rights case law on Article 8), including case-law and scholarly analysis in nine countries, both common law and continental (USA, UK, Canada, Germany, the Netherlands, Poland, Italy, the Czech Republic and Slovenia; *ibid*., pp. 490).[89] The main

88 Parts of the description of this Section are taken from the Koops et al. (2017) paper with the permission of the other authors of the paper.

89 This typology claims to overcome (or at least lessen) the drawbacks of existing typologies of privacy, which are often embedded in a single legal culture (e.g. US) so that they are not necessarily generalizable outside of their own jurisdiction; they usually draw from the work of a handful prominent and largely US-based scholars, understating important cultural variation; and, moreover, they are not based on clear-cut distinctions, resulting in a list of relevant privacy aspects rather than a typology.

idea was that the identification of various objects of protection of the right to privacy (as it has developed in law in the last 120 years or so), assisted by theoretical privacy scholarship from each jurisdiction, can help distinguish the most relevant types of privacy, while preserving important cultural variation.

In this Section, I will first explain the developed three-dimensional model of privacy types, followed by a description of the identified types of privacy.

This typology of privacy contains two primary dimensions. Drawing from Westin's four states of privacy (but modifying his categorisation with additional insights), the horizontal axis moves along a spectrum from the personal or completely private zone to intimate, semi-private, and public zones (Koops et al., 2017, p. 545). Importantly, the terms 'public' and 'private' do not simply refer to *spaces* but rather to the nature and character of inter-personal association (if any). Thus, the ideal types of each identified type of privacy differ in their degree of *privateness* by reference to their degree of social engagement or isolation, the nature of the engagement and the pre-existing or developing relationships between participants, and the nature of the space in which the engagement takes place.

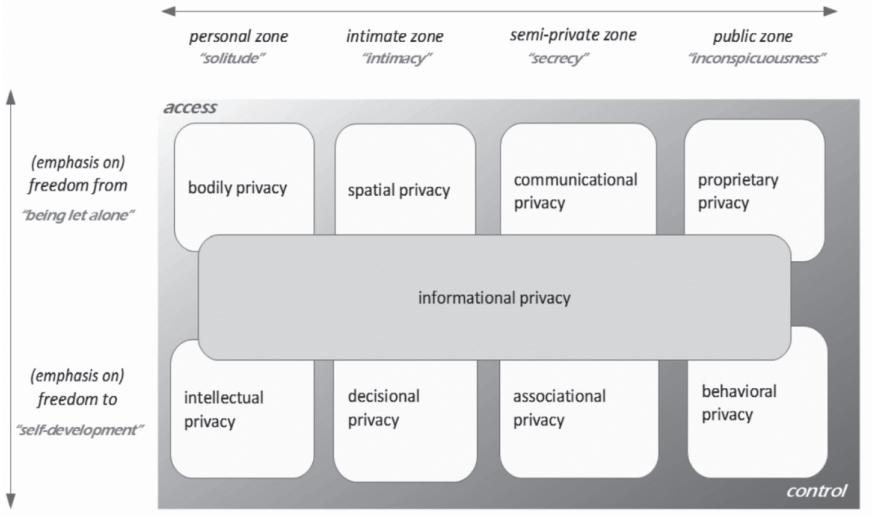


Figure 3.1: *The nine privacy types from the typology of privacy by Koops et al. (2017, p. 484)*

The *personal zone* is typified by solitude or isolation. The *intimate zone* is characterized by a shift towards social engagement, albeit limited to intimate partners, family members, and close friends, as well as activities that take place in private and fenced-off spaces, such as the home where people share their life with intimate partners and family.

The *semi-private zone* includes social interaction with a wider range of actors, including acquaintances, work colleagues, and professional relationships (e.g., interacting with a doctor or a sales-person), and activities that occur in more quasi-public space. The *public zone* is typified by activities occurring in public – for instance, in a public square, on public transportation, or on publicly accessible electronic platforms – where the privacy interest is characterized by the desire to be inconspicuous despite being physically or virtually visible in public space. This zone sits at the edge of the outer layer of privacy and social life.

On the vertical axis, the spectrum of negative and positive freedom is employed, which can be characterized by the key terms of 'being let alone' (emphasis on negative freedom) and 'self-development' (emphasis on positive freedom). Although there is no sharp boundary between *freedom from* and *freedom to*, presenting the ideal types of privacy along this spectrum aids the understanding of the variation that occurs within privacy, according to Koops et al. (*ibid*., p. 565).

Furthermore, there is a third dimension that follows from distinctions drawn in the literature between restricted access and subsequent control after access has been granted. This dimension is not independent from the other two, but rather combines both in the sense that restricted access is associated more (although not exclusively) with the private than with the public zone, and more with negative freedom than with positive freedom, while control after access is more significant in the semi-private and public zones and has more the character of a positive freedom (self-determination). Thus, this dimension runs across both axes from upper left to lower right. For example, any privacy interest in a person's behaviour in public space has more to do with controlling the use of information about that activitity than it does with restricting access (since some access has already been granted by the nature of the space itself). On the other hand, bodily privacy is typically (although not always) a question of access, rather than control.

These concepts are presented as situated on a continuum from restricted access – meaning *exclusion*, or the right to exclude access to persons, places, things, persons, or information about any of these – to control over the subsequent use of information/persons/places/things after some access, explicit or implied, has been granted. At one end of this spectrum, privacy protects the right of a person to exclude access to her body, home (and other private places), and property, as well as personal thoughts and processes of the mind. Moving towards the other end, privacy may protect the confidentiality of communications, the secrecy of records, and control over the use of personal data (even after access has been granted) as well as activities occurring in

semi-public or public zones, because access can be more readily inferred based on the public nature of the space (i.e., access cannot be withheld from public activities, in a practical sense).

Within this model, Koops et al. identified eight primary types of privacy with informational privacy (the ninth type) as an overlay of all of the other types of privacy that overlaps, but does not coincide, with the eight basic types. These types of privacy are 'ideal' in a Weberian sense – that is, they are 'formed by the one-sided *accentuation* of one or more points of view' (Weber, 2017, p. 90; as cited in Koops et al. 2017, p. 495; emphasis in original). This can be explained through the analogy of the magnifying glass, which magnifies the features of the ideal types to the extreme (Bailey, 1994, p. 19). As such, ideal types are an analytical tool that demonstrate certain characteristics very clearly and are useful to think with and help make sense of the world around us (Nippert-Eng, 2010, p. 5). The identified ideal privacy types are characterized as follows.

Bodily privacy is typified by individuals' interest in the privacy of their physical body, where the emphasis is on negative freedom – being able to exclude people from touching one's body or restraining or restricting one's freedom of bodily movement.

Spatial privacy is typified by the interest in the privacy of private space, by restricting other people's access to it or controlling its use. As such it refers to the protection of the privacy of people in relation to the 'places where they enact their private life' (Koops et al., 2017, p. 516). Although spatial privacy may extend beyond the intimate zone, its ideal type is best situated in this position because of the role that private space plays in preventing access to intimate activities. The home is the prototypical example of the place where spatial privacy is enacted, closely associated with the intimate relations and family life that take place in the home. Nevertheless, spatial privacy can also refer to other places, such as hotel rooms, workplaces, garages, even vehicles and computers (see Chapter 6 on ECtHR case law).

Communicational privacy is typified by a person's interests in restricting access to commnications or controlling the use of information communicated to third-parties. Communications may be mediated or unmediated, which involve different ways of limiting access or controlling the communicated messages.

Proprietary privacy (referring to property-based interests, rather than Allen's (2011) reference to image management and reputational privacy) is typified by a person's interest in using property as a means to shield activity, facts, things, or information

from the view of others. For example, a person can use a purse to conceal items or information they prefer to keep private while moving in public spaces.

Intellectual privacy is typified by a person's interest in privacy of thought and mind, and the development of opinions and beliefs. While this can have important associational aspects, it is suitable as an ideal type of the personal zone, as the mind is where people can be most themselves.

Decisional privacy is typified by intimate decisions, primarily of a sexual or procreative nature, but also including other decision-making on sensitive topics within the context of intimate relationships. As with spatial privacy, decisional privacy as an ideal type within the intimate zone is closely related to family life.

Associational privacy is typified by individuals' interests in being free to choose who they want to interact with: friends, associations, groups, and communities. This fits in the semi-private zone since the relationships often take place outside strictly private places or intimate settings, in semi-public spaces such as offices, meeting spaces, or cafés.

Behavioral privacy is typified by the privacy interests a person has while conducting publicly visible activities. These relate to Westin's states of anonymity and reserve and to Cohen's concerns with exposure and transparency. In contrast to items people carry with them in public (which can be hidden and therefore to some extent excluded from others' view), one's personal behavior in public spaces is more difficult to exclude others from observing, and thus is an ideal type of privacy where the need for control or, better, discretion after access has been granted is most pressing. 'Being oneself' in public can only be achieved if others respect privacy through civil inattention, but otherwise control can only be exercised by trying to remain inconspicuous among the masses in public spaces.

Finally, as mentioned above, informational privacy[90] is conceptualised as an overarching aspect of each underlying type, typified by the interest in preventing information about one-self to be collected and in controlling information about one-self that others have legitimate access to. Despite the frequency at which informational privacy has

90 Also referred to as 'data privacy'. Here the term 'informational privacy' is used since the privacy interest ultimately sees to data that may say something about a person, hence information. While the *right to privacy* often covers personal data, the *type of privacy* thus is more concerned with personal information.

been classified as a separate type of privacy alongside, and thus on the same level as, other types, Koops et al. (2017, p. 568) think it should be represented instead as an overarching aspect. This conclusion is informed by Blok's (2002) argument that informational privacy is better understood as the 'other side of the coin' rather than a separate type. After all, each ideal type of privacy contains an element of informational privacy – that is, a privacy interest exists in restricting access or controlling the use of information about that aspect of human life. For instance, bodily privacy is not limited to restricting physical access to the body, but also to resticting and controlling information about the body (e.g., health or genetic information). Since informational privacy combines both negative freedom (excluding access to information) and positive freedom (informational self-determination), which can regard information relating to any of the four zones of life, informational privacy is depicted in our model as an overlaying concept that touches each of the primary types.

3.3 Privacy mechanisms

In this Section, I will examine privacy mechanisms – that is, ways in which privacy is sought and, sometimes, achieved.[91] In other words, I ask the question: *how* is privacy gone about and achieved? However, privacy mechanisms consist of a wide range of techniques or tools, including social, legal, and technical (or architectural). In this Section, I will focus on the various social mechanisms of seeking privacy or 'privacy behaviours' (Nippert-Eng, 2010, p. 5) such as secrecy, seclusion, behavioural mechanisms such as civil inattention, discretion, reserve and inconspicuousness, Altman's boundary management theory and Nissenbaum's contextual integrity. In order to answer the main research question in this dissertation – how should privacy in public space be conceptualised and, thus, regulated? – one must namely examine those privacy mechanisms that have been most relevant for achieving privacy in public and are now said to be at risk. As several scholars have pointed out, these mechanisms largely consist of social mechanisms (e.g. Altman, 1975; Nissenbaum, 1998; Paton-Simpson, 2000; Westin, 1967). As Westin (1967, p. 32) put it: 'The manner in which individuals claim reserve and the extent to which it is respected or disregarded by others is at the heart of securing meaningful privacy in the crowded, organization-dominated settings of modern industrial society and urban life, and varies considerably from culture to culture.'

However, this does not mean that I do not engage with other mechanisms at all. I will examine the legal mechanisms in Section 4 on the right to privacy (and the human

91 As such, there is a slight overlap between this Section and the section on the phenomenon of privacy in 2.1.1.

right to respect for private life in the ECHR in Chapter 6). Furthermore, technical mechanisms, such as privacy (or data protection) by design, are clearly important in the context of privacy in public space. However, this issue requires a particular focus on technology (going beyond the scope of this dissertation) and further work in this rather new field is, however, very much needed.[92] As such, I only briefly discuss such these in Chapter 7, in connection to possibilities for regulation through architecture and code.

According to Nippert-Eng (2010, p. 25), there is a continuum between the most personally active and passive ways in which we obtain privacy. At one end, there are the concealing or dissimulating behaviours associated with secrecy, which can be described as the most active of techniques through which we achieve privacy. At the other end, there is non-interest of others associated with social ambivalence and/or proper etiquette, which are among the more passive ways of achieving privacy. Furthermore, privacy behaviours can be distinguished among those with which the individual makes oneself inaccessible to others as much as possible (such as seclusion and secrecy) and others with which the individual allows for a certain limited level of access to the self by others (such as reserve). Privacy mechanisms can also involve different types of social units, including individuals, families, and mixed or homogenous groups.

3.3.1 Seclusion

Privacy has traditionally been understood as a process of withdrawal from others (Hughes, 2012, p. 811). As such, solitude was seen by several authors as a foundational aspect of privacy (Gavison, 1980; Prosser, 1960, p. 389). This is so because solitude provides the individual with an opportunity 'to anticipate, to recast, and to originate' (Park 1921, p. 231). Similarly, Westin (1967, p. 40) considered that contemplation achieved through (privacy as) solitude enables the individual 'to integrate his experience into a meaningful pattern and to exert his individuality on events'. And solitude is essential for the individual to carry out such self-evaluation. In scholarly privacy literature, solitude is thus connected to bodily privacy (referring to physical inaccessibility and separation from others), spatial privacy (corresponding with the term seclusion and referring to physical distance or possession of space) and intellectual privacy (referring to calm, peace and tranquillity, and sanctuary connected to the

92 Research in this field is being undertaken by several scholars at the intersection between law and engineering, including: (2018), Koops and Leenes (2014), Cavoukian (2010). See also Hildebrandt, M. (2019). Counting as a Human Being in the Era of Computational Law (COHUBICOL). Retrieved March 26, 2019, from https://www.cohubicol.com/.

freedom of thought). Private life, indeed, has certain aspects that, by their nature or otherwise, allow a total isolation (such as diaries and domiciliary life) or do not suppose any relation with other persons (Mantovani 2011, p. 584; as referred to in Koops et al., 2017, p. 547).

Seeking seclusion is thus a means of achieving privacy *from* others, referring to erecting physical barriers to sight, sound, touch, and smell (Marshall, 1972, p. 94). When a person seeks seclusion, she desires to be unreachable by others (e.g. that others do not see what she does in the locked bathroom). Oftentimes a person also desires seclusion from external stimuli, such as smells from neighbours' cooking and noise from the street. As such, seclusion is most commonly sought and found at home (especially if one is living alone) or in certain places of the home (e.g. the bathroom, private bedroom and attic). Persons can lock their doors, disable their door-bells, and close the windows and shutters. They can also choose to live in a secluded area so as to achieve a higher level of solitude, even when venturing outside of their homes. While seclusion can also be sought in more populated public areas, for instance in a meadow at the outskirts of a town, achieving it remains a matter of luck, as one cannot prevent others from having a walk in the meadow at the same time.

While privacy should not be equated with seclusion (contrary to Gavison, solitude is not 'perfect privacy'; Gavison, 1980, p. 428), as it is possible for one to enjoy privacy while not necessarily having solitude, seclusion nevertheless remains an important privacy mechanism. At certain times, a person indeed needs complete solitude, most notably for intellectual and spiritual contemplation as well as the performance of certain basic bodily functions.

3.3.2 Secrecy

Another way to seek and achieve privacy is through secrecy. According to Nippert-Eng (2010, p. 24), secrecy is a way of achieving privacy whenever individuals (or groups) wish to ensure that the most private and important of their matters are kept hidden. Secrecy is thus a means to an end, 'a process in which we actively work to manage our private matters' (*ibid*., p. 24). By employing secrecy, we leave little about our privacy to chance and others' agendas. As such, it is one of the most active techniques through which we seek privacy.

Similarly to solitude, secrecy is also a common understanding *of* privacy (rather than merely a means of achieving it; for more see Solove, 2002, p. 1105). Within this perspective, however, some have argued that secrecy should be distinguished from privacy on the basis of the morality of behaviours to which they refer, where

secrecy is used to conceal something negatively valued by the excluded audience (and sometimes by the perpetrator herself) (Shils, 1966; Warren & Laslett, 1980). As such, privacy refers to a legitimate denial of access (to an act the existence of which is generally known), while secrecy relates to the denial of access that is illegitimate. This view, however, seems too narrow, limiting the function of privacy to concealed enjoyment of socially acceptable behaviour and forgetting about its role in autonomy and identity development, where experimentation sometimes includes socially unacceptable behaviour.

Indeed, as sociological scholarship has shown, anything can be a secret; the form is analytically distinct from its content. As Bok (1989, p. 5) put it: 'A path, a riddle, a jewel, an oath – anything can be secret so long as it is kept intentionally hidden, set apart in the mind of its keepers as requiring concealment.' I thus understand keeping secrets (in this broad understanding) as one possible means (or mechanism) of achieving a certain level of privacy, especially for – but not limited to – those aspects of one's private life that are held in disrepute by the society or others that one is, for one or other reason, not willing or capable to share with anyone or the majority of people.

Probably the most significant aspect of keeping secrets is the selectivity with which we share them. We can distinguish between keeping secrets *with* and keeping secrets *from*, as they are intentionally disclosed to and concealed from specific individuals at specific times and in specific ways. Secrets can be solely known or shared with others.[93] As such, keeping secrets is simultaneously inclusive and exclusive, an effective measure of the social distance between individuals (Nippert-Eng, 2010, p. 27). On the one hand, a secret reinforces and heightens intimacy among those who share it, and, on the other, it increases the sense of being distinct (or completely cut off) from those who do not share it. One could describe the operation of a secret withheld from others as a brick in the wall between its holder(s) and all potential sharers (*ibid*., p. 30). This may or may not be a good thing – it can be both detrimental to relationships, but it can also allow happy and peaceful cohabitation. Furthermore, the keeping of secrets is connected to the presentation of our selves to others and, more broadly, to identity-building. Persons not only wish to hide matters (both in terms of thoughts and material things) that society finds unacceptable, they oftentimes wish to hide matters that would simply show them in a bad or embarrassing light. And, considering

93 According to G. Simmel (1964, pp. 317–329) every type of social relationship is defined by the expected degree of secrecy and secret sharing – what he terms 'knowledge reciprocity' – associated with it.

the importance of self-presentation for identity-development (as discussed in Section 3.1.1), the keeping of secrets is an important mechanism to have at one's disposal.

However, as Bok (1989, p. 19) pointed out, secrecy also confers power:

> 'To be able to hold back some information about oneself or to channel it and thus influence how one is seen by others gives power; so does the capacity to penetrate similar defenses and strategies when used by others. To have no capacity for secrecy is to be out of control over how others see one. … To have no insight into what others conceal is to lack power as well.'

Conflicts over secrecy are thus also 'conflicts over power: the power that comes through controlling the flow of information' (*ibid.*). The 'owner' (or 'owners') of the secret has the power – she can either keep the secret or disclose it, with consequences for the privacy of everyone involved. Namely, keeping secrets also helps avert any anticipated negative social consequences associated with their disclosure. According to Zerubavel (2006, p. 41), 'secrecy … tacitly stabliz[es] existing power structures.' It does so by protecting the behaviors of those who are powerful enough to demand and maintain the secrecy surrounding their acts.[94] But challenge the secrecy and one challenges the very distribution of power and nature of the relationships that enabled it. As such, disclosing a secret is also an important tool used in organisations by individuals who wish to dissociate them selves from other members, particularly when they disapprove of what those members stand for, such as in the case of whistle-blowers (see e.g. Zerubavel, 2006).

3.3.3 Civil inattention, reserve and inconspicuousness

Civil inattention, reserve and inconspicuousness are a part of a myriad of complex social rules and practices that people employ, especially in order to minimise the risks of appearing in public, providing a level of balance between practicality, curiosity and privacy (Paton-Simpson, 2000, p. 236). These behavioural mechanisms are, of course, deeply embedded in social norms, which vary in time and place. In this Section, I will briefly discuss those social practices that are broadly found in the West nowadays (although to differing extents).

94 Nippert-Eng (2010, p. 51-2) gives the example of a secret shared between a victim of incest and her parents. According to Nippert-Eng, the fact that this secret has been kept for so long is a clear indication that the mother and the father continue to have the upper hand in their relationships with their daughter. The daughter's threat to finally tell is a threat to upend those relationships, to redistribute power throughout the family in a way that would be anathema to those who currently possess the lion's share of it.

Reserve refers to the self-presentation barriers that people employ as a privacy preserving tactic, when they venture out in public.[95] This creates 'mental distance' (G. Simmel, 1964), which is found in sorts of relationships under rules of social etiquette, with the role of protecting the personality (also discussed in Section 3.1.1).

This conscious effort on the individual's side is aided by effort on the side of others, found in the form of discretion (sometimes called civil inattention). According to Goffman (1966, p. 85), civil inattention is a form of polite recognition of strangers, manifesting itself in brief nods or other signs of acknowledgement by a respectful modesty not to intrude where one does not belong. In other words, it refers to the effort of others to stay away from the knowledge of all that we do not expressly reveal to them. It does not refer to anything in particular that other are not permitted to know (like a secret), but to a quite general discretion in regard to the personality (G. Simmel, 1964). One should thus not only not stare at or photograph a physically injured bystander (although one should take sufficient notice of others in order to be able to offer assistance to those in need) but should not stare at others in general (again, unless their behaviour specifically calls for attention). Notably, civil inattention does not distinguish in a binary manner between private and public activities, as privacy theory and law often do (see also Chapter 6 on the distinctions between public and private activities in ECtHR case law).

Another type of privacy mechanism, closely related to reserve and discretion, is found in the myriad of ways through which one becomes inconspicuous. Inconspicuousness refers to the fact that one is not readily noticeable, despite being among others. According to Goffman, civil inattention is in fact a mechanism of achieving inconspicuousness. That is, civil inattention does not only involve disinterestedness without disregard of the individual *offering* civil inattention, it also includes a requirement on the part of the individual who *enjoys* civil inattention (Sharon & Koops, 2019 forthcoming). In other words, if there is a social obligation to extend civil inattention to others, this is not a natural right but one that is acquired by behaving in a manner that summons or deserves civil inattention as an adequate response. One thus needs to make oneself 'disattendable' – not give others cause for a particular need for attention (*ibid*.). Whether one sees this as a part of the process of civil inattention or not, is not essential here. What is important is that there are several additional active mechanisms through which one can achieve being inconspicuous in public,

95 Interestingly, according to Westin (1984), reserve is enacted by others rather than by the person herself, and refers to psychological distance that others employ to respect privacy of others, when these indicate a desire for withdrawal or simply because of social conventions of propriety.

including dressing and behaving within the norm (in the sense of norms of propriety) so as not to attract attention (rather than dressing, for example, like a punk in order to show your disregard for the establishment). A person may also involve material props for this purpose, such as newspapers, books or sunglasses, which act as barriers to perception.

3.3.4 Boundary management

The idea of privacy as boundary management (Altman, 1975, 1976) has gained much traction recently. Many contemporary scholars (e.g. Hughes, 2012; Nippert-Eng, 2010; Petronio, 2002; Steeves, 2009) have based their conceptualisations of privacy on Altman's theory that privacy is an interpersonal boundary control process.

Altman placed special significance on Westin's insight that people seek a balance between closedness and openness in relation to others and that too much or too little separation from others is an undesirable state of affairs. Rather than placing privacy and social interaction at opposite poles, however, Altman conceptualised privacy as a dialectic and a non-monotonic concept,[96] as opposed to the traditional view of privacy of shutting off the self from others (1975, p. 11).

Social interaction is a continuing dialectic between forces driving people to come together and to move apart. Accordingly, privacy is a continually changing process, which reflects a momentary ideal level of interpersonal contact, ranging from wanting to be accessible to others, to wanting to be alone. A corollary of the dialectic idea is the idea of the non-monotonic quality of reactions to social interaction – since too much or too little privacy is unsatisfactory, people always seek an optimal level of social interaction. 'Ideal' privacy is, thus, a position on a continuum of desired interaction (Altman, 1976, p. 12). In accordance with these ideas, privacy for Altman is a boundary regulation process, a flexible barrier or boundary between the self and others (*ibid*., p. 13). Privacy is defined as selective control of access to the self (or to one's group) by which a person (or group) makes oneself more or less accessible and open to others (*ibid*., p. 8). Altman uses the example of a cell-membrane, whose boundary properties change in accordance with the state of the external and internal environment. A person (or group)[97] thus makes use of privacy mechanisms similarly

96 Based on Simmel's work on the dialectic quality of social exchange, which posits that without such interplay, social existence itself would not be viable.

97 Privacy mechanisms can also involve different types of social units, including individuals and families, mixed or homogenous sex groups (Altman, 1975, p. 11).

to the cell membrane that becomes more or less permeable, depending on the desired viable level of functioning.

More specifically, the mechanisms and dynamics of privacy include verbal and para-verbal behaviour, non-verbal behaviour, environmental (territorial) behaviour, and responses based on cultural norms and customs (Altman, 1976, p. 7). According to Altman these mechanisms function as an integrated system, sometimes substituting for each other, sometimes complementing one another, at other times conflicting with each other. In this sense, privacy mechanisms themselves are dynamic and responsive to the context. Privacy regulation therefore involves a complex feedback system in which resources (privacy mechanisms) are mobilized to achieve a desired level of privacy.

Verbal and para-verbal mechanisms refer to *what* is said and *how* it is said, including language styles, vocabulary selection and diversity, pronunciation and dialect, voice dynamics and speech rate. Non-verbal behaviour involves the use of various parts of the body as a privacy mechanism, such as covering the face or averting direct eye contact. Environmental privacy mechanisms refer to the ways in which physical environments can be used to regulate privacy. More specifically, they relate to how people use doors, windows, furniture arrangements and the design of (private and public) space. For example, keeping doors among rooms closed or having one's own room, where one can be alone, is a way to achieve interfamilial privacy.

Another important environmental privacy mechanism according to Altman, is the use of 'personal space'. Personal space refers to an *invisible bubble* – the area immediately around the body, intrusion into which leads to discomfort or anxiety (Altman, 1975, p. 6; based on the work of Sommer 1969; Hall 1966). As such, it is an invisible boundary between the self and others, which is *attached* to the self, so that it is carried everywhere one goes. Like all privacy mechanisms, it is a dynamic process that permits differential access to the self as situations change. It is important to note that personal space does not translate into physical distance from others alone. Rather, personal-space intrusion can result from overly close physical distance, inappropriate body positions, and behaviours that result in excessive symbolic intimacy (e.g. staring into one's eyes or other body parts, breathing on another or making one smell them due to proximity) (Altman, 1975, pp. 86–87; following Leibman 1970).

According to Altman, the main function of privacy is its role in the construction of one's identity. Privacy mechanisms thus define the limits and boundaries of the self, so that when the permeability of those boundaries is under the control of the person,

a sense of individuality develops (*ibid*., p. 50). Consequently, it is not the inclusion and exclusion process itself that is key; what is key is the *ability* to do so, which contributes to self-definition: 'If I can control what is me and not me, if I can define what is me and not me, if I can observe the limits and scope of my control, then I have taken major steps toward understanding and defining what I am' (Altman, 1976, p. 26).

3.3.5 Contextual integrity – norms of information flow

Nissenbaum developed her normative account of privacy in terms of contextual integrity in light of technological advances (including, profiling, data mining and RFID tags) at the break of the century (1997, 1998, 2004, 2010). She submits that a right to privacy is neither a right to secrecy nor a right to control personal information but 'a right to appropriate flow' of personal information (Nissenbaum, 2010, pp. 1–2).

A key aspect of contextual integrity is that 'there are no arenas of life *not* governed by *norms of information flow*' (Nissenbaum, 2004, p. 137; emphasis in original). 'Almost everything – things that we do, events that occur, transactions that take place – happens in a context not only of place but of politics, convention, and cultural expectation' (*ibid*.).[98] The activities that people engage in thus take place in a plurality of distinct contexts. These contexts are wide-ranging – they can refer to 'spheres of life', such as education or politics, or they can be finely drawn so as to refer to conventional routines of attending a friend's wedding and going to the dentist. Each of these contexts involves a distinct set of norms, which governs its various aspects, such as roles, expectation, actions, and practices. These norms can be rather explicit and specific (e.g. attending church services or court proceedings) or implicit, variable and incomplete (or partial; e.g. in different types of friendship).

Contexts are rooted in numerous sources, such as history, culture, law and convention. However, norms that are present in most contexts are those that govern information, in particular information about the people involved in the contexts. Nissenbaum divides these information norms in two types: norms of appropriateness and norms of flow or distribution. When both types of norms are maintained, 'contextual integrity' is upheld; on the contrary, contextual integrity is violated when either of the norms is violated. Contextual integrity is thus seen as a key benchmark for privacy – if at least one type of the informational norms has been violated, then privacy has been violated too (although the violation may nevertheless be justified, if another, more serious or urgent value was at stake; Nissenbaum, 2004, p. 138).

98 This phenomenon of distinct types of contexts of firmly rooted in common experience and has been profusely theorised by philosophers, social scientists and theorists (see, e.g. Walzer, 1983).

Norms of appropriateness dictate what information about persons is appropriate (or fitting) to reveal in a particular context. 'Generally, these norms circumscribe the type of nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed' (*ibid*.). For instance, while we may fully reveal our romantic entanglements to our friends, we might not want to reveal our financial situation to them; on the contrary, we would only reveal financial information to the bank but not our romantic life. This is connected to the more general notion that persons need to be able to share information discriminately (Rachels, 1984) in order to be able to develop and maintain different relationships with different people in different contexts. As Schoeman (1992, pp. 72–73) put it:

> 'A person can be active in the gay pride movement in San Francisco, but be private about her sexual preferences vis-à-vis her family and co-workers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?'

The other set of norms governs the flow or distribution of information, that is, the movement or transfer of information from one party to another or others. This set of norms (based on Walzer's concept of 'complex equality'; 1983) adds distributive principles (or distributive criteria) to the notion of contextual integrity. 'What matters is not only whether information is appropriate or inappropriate, but whether its distribution, or *flow*, respects contextual norms of information flow' (Nissenbaum, 2004, p. 141). Personal information revealed in a particular context is, namely, always tagged with that context and never 'up for grabs', as it is sometimes argued. Also, norms of appropriateness and norms of flow need not correspond. For instance, while norms of appropriateness in friendship might be very much open-ended, the same does not apply to norms of information flow in this context, which are rather substantial. Confidentiality, as one example of the norms, is generally the default – friends expect that what they say to each other (and what is inferred from the said) will be held in confidence and not arbitrarily spread to others.

In view of this theory, existing informational norms are put forward as benchmarks for privacy protection. As such, one might argue that the theory endorses entrenched flows that might stand in the way of improvement, that it preserves the status quo in detrimental ways. Nissenbaum recognises this critique and posits that her theory does not fixate existing norms, instead it establishes a default to which a norm applies,

barring counter-arguments why the context has changed. Furthermore, the theory might be criticised by positing that it does not have prescriptive value for the use of new technologies, as it is so tied to practice and convention. Nissenbaum, however, points out that with new technologies one needs to see how they change existing contexts, and should not (as they often are) be framed as a new context.

4. VARIATIONS ON A RIGHT TO PRIVACY: PRIVACY AS A PERSONALITY RIGHT, AS A HUMAN AND FUNDAMENTAL RIGHT AND PRIVACY AS THE RIGHT TO PROTECTION OF PERSONAL DATA

The analysis of the various conceptions of privacy above needs to be complemented with another type of theoretical conceptualisation – the right to privacy. The right to privacy has shaped the (Western) societies we live in and the persons we are so much that we have a tendency to view these rights as part of the natural fabric of our existence. There is, however, nothing natural, universal or necessary about our conception(s) of the right to privacy, rather, it is a choice that needs to constantly be made (and that we keep on making). A better way to think about the right to privacy is to consider it a social and political achievement, the existence of which contributes to the definition of a political and legal system, as a mode of political coexistence (Periñán, 2012, p. 201).

However, there seems to be a serious lack of understanding of the right to privacy, resulting in calls for more classification (e.g. Blok, 2002) as well as for the trimming of the right (e.g. van der Sloot, 2015). Indeed, the right to privacy, at least as a unitary conception, cannot be traced back to an originating, single point in time and space. It is not found in a single document or code, rather it is a 'patchwork of legal provisions' (Strömholm, 1967, p. 76), found in constitutional, criminal, civil and administrative law. Some thus prefer to talk about 'privacy law' rather than the right to privacy (Allen & Rotenberg, 2016), while others refer to 'rights to privacy' (e.g. Scanlon, 1975).[99] Moreover, the human and fundamental right to privacy, as found in national constitutions and supra- or international legal documents, is often considered too broad and vague, tightly entangled and partly overlapping with other rights (particularly with the right to data protection). This is only exacerbated by the fact that there are major terminological discrepancies in the field of privacy law across

99 In this dissertation I will use the term rights to privacy, when speaking of privacy law in general, and a right to privacy (or private life), when speaking of a right in particular.

states and many countries provide what can be regarded as privacy protection through different notions (Strömholm, 1967, p. 21).[100] Our modern conception of the right to privacy is also shaped in response to new technologies and practices by business and government. As such, the right is dynamic and developing in time. Our persistent inability to sufficiently address these issues has led some to describe the right to privacy as a kaleidoscopic right: 'Modify the angle of observation, and its physiognomy is altered as if it were not exactly the same right in each position' (Picard, 1999, p. 58).

If the conceptual obscurity of privacy is at worst a cause of vexation and, at best, a great source of writing topics, it can result in more serious and tangible consequences when connected to a legal right. Dworkin (1978, p. 114) thus put it well: 'The difficulty of defining privacy is even more unsatisfactory to the lawyer than to others.' Given this 'extraordinarily complex and confused situation with the right to privacy' (Picard, 1999, p. 58), the best method to provide a sufficiently clear account of what the right to privacy may be, at least in (continental) Europe and what it may and should further develop into, is to show how this right was initially formed and how it subsequently evolved. According to Dworkin (1978, p. 113), the lawyer must thus ask herself three questions: first, what is the meaning of privacy; second, to what extent is this concept already protected in law; and, finally, if such protection is not adequate, what kind of law reform is required.

Therefore, in this Section I will first examine the development of the right to privacy, giving a brief account of the various origins of the right. Second, I will offer a brief account of the development of the right to privacy in the United States of America (U.S.). While the focus of this dissertation is on (the right to) privacy in Europe, this particular account of privacy has been so influential that is nowadays seen as the origin of privacy as a legal value not only in the U.S. but in the West in general (Strömholm, 1967, p. 25). I will then examine privacy as a type of personality right and then its emergence as a human (and fundamental) right. Since I will discuss the legal framework of right to respect for private life (Article 8) as set up by the European Court of Human Rights (ECtHR) in a separate Chapter (Chapter 6), I will examine the right to privacy as a human right in Europe only briefly. For reasons given in the

100 The French use the term 'private life' (*vie privée*), the Germans 'the right to informational self-determination' (*informationelle Selbstbestimmung*), in Italy they have both a concept of 'privacy' (which usually refers to data protection) as well as 'riservatezza' (the term often used for privacy, literally: reservedness). The Nordic Conference of Jurists on the Right to Respect for Privacy in 1967 went ahead with a discussion using the term 'right to privacy' as encompassing related legal notions developed in Europe under other names, and eventually concluded by encouraging the adoption of laws establishing a general right to privacy (González Fuster, 2014, p. 39).

Introduction, I will not examine the specific and entangled relationship of the right to privacy and the right to data protection in the European legal framework. This thorough examination of the various aspects of the right to privacy will help me to develop a theoretical and legal concept of the right to privacy in public space, with a focus on the continental European legal framework in mind.

4.1 A brief account of the origins of the right to privacy

As mentioned above, the right to privacy did not emerge at a given moment in time and space but was shaped in a piecemeal manner lacking unity to this day (Picard, 1999, p. 49). It is thus valuable to look at certain, though in no case exhaustive, early emanations of the right to privacy. In this sub-section I will examine examples from ancient Roman law and England from the Middle Ages to the 20th century.

According to some, privacy as a legal value is a quite recent development, related to the political and social principles of the French Revolution. In the newly emerging relationship between the citizen and the modern state, the individual was acknowledged as a whole – as the holder of the personal sphere of life, which then needed to be legally protected (Constant, 1980; Periñán, 2012, pp. 188–189; Picard, 1999). And, yet, as others have noticed, the roots of privacy as a legal value are much older than that (Periñán, 2012; Picard, 1999, p. 52). One of the earliest (Western) manifestations of privacy as a legal value can be found in Roman law.[101] There are no specific legal declarations of a right to privacy in Roman law and words such as *privacitas* or *personalitas* are not used at all. Nevertheless, since legal ideas are not natural facts waiting to be uncovered (Ibbetson, 2001, p. v), the existence of these legal values can be inferred from the shape of classical Roman law. In this legal system, the main means of what can be seen as one of the earliest manifestations of the right to privacy was the *actio iniuriarum* (Periñán, 2012, p. 190). This *actio* provided for redress for aggressions against non-physical aspects of the personality (alongside redress for physical injuries; see Zimmermann, 1996). These aggressions were considered a private or personal attack on a person's honour, where *dolus* (bad intent) was required. The *actio* was thus applied in cases of defamation and other situations, such as offences against decency, especially regarding women and youth, or against one's right to a private residence (*domicilium*), protecting from any attack on one's private property

101 There are quite possibly other and earlier manifestations of the right to privacy but I will limit my historical account to its manifestations in Roman law, which has had a large and lasting impact on the continental European legal systems.

preventing the owner from using it.[102] In ancient Roman society, however, no legal protection of the secrecy of communication existed, although a corresponding social value might have existed (Periñán, 2012, p. 194).

Following the exceptional legal developments found in the legal system of ancient Rome, no particularly obvious roots of the right to privacy are detected until the Middle Ages in Europe. England is commonly considered the 'cradle or birthplace of modern privacy' (Ariès, 1989), so that it is not surprising that subsequent manifestations of the right to privacy are first found there.[103] Vincent (2016, p. 3) points to the different types of legal disputes over matters of privacy in medieval London. In the early 14th century, there was a possibility (although in practice a last resort) to bring forward to the *London Assize of Nuisance* not only an action of trespass (giving householders recourse against the physical invasion of private space) but also an action against nuisance – referring to other types of behaviour by inhabitants of neighbouring buildings that diminished the value of the householder's occupancy of his premises. For instance, a neighbour's incessant peering onto another person's garden from a watchtower or through one's window. This early stage of the legal history of privacy shows a strong association of privacy with property, including a basic association between privacy and the occupancy of a domestic residence (Allen & Rotenberg, 2016, p. 43; Vincent, 2016, pp. 6–8). This idea became enshrined in English law in 1604 with the ruling that 'the house of everyman is his castle', which was 'already a hoary cliché of English common law' by 1700 (Vincent, 2016, p. 33; referring to the statement of Amanda Vickery).

Aside from nuisance laws, the early manifestations of the right to privacy can also be found in defamation laws of the 16th century (Periñán, 2012, p. 198). The physically-based nature of the English common law in Middle Ages was not in favour of creating an offence which rested on mere words, rather it was concerned with tangible actions and results of, for example, assault, theft and murder. However, in 1507, when the

102 This foundation was also recognised in early privacy tort case law, more specifically in the 1905 Pavesich case (as cited in Allen & Rotenberg, 2016, p. 43): 'Under the Roman law, "to enter a man's house against his will, even to serve a summons, was regarded as an invasion of privacy." … This conception is the foundation of the common-law maxim that "every man's house is his castle."'

103 While this is a common perception, other European countries also likely had some legal protection of privacy interests in medieval times. For instance, Norway seems to have established a law on the secrecy of communication already by the early 1300s. It concerned 'letter-breaching', which was a punishable offense of breaking the seal on letters addressed to someone else. Moreover, medieval Norway letters were often safeguarded and conveyed in carved wooden boxes that could be securely closed (Nunnally, 2005, p. 1140).

first common law defamation case on record was brought, the King's Court decided that mere words indeed can impact the honour of a man as much as, or even more so, than physical attacks.[104] Three categories of defamation have thus emerged at the time: (1) words accusing someone of a crime; (2) words accusing someone of being incompetent at their job and (3) words accusing someone of having a particular disease. Until 1660, common law did not draw a clear distinction between defamation that was spoken or that which was in writing. However, defamatory words in writing were often punished with harsher sentences. Privacy in Europe in the Middle Ages was thus recognized through the right to a private residence (property) and the right to honour (Ibbetson, 2001). It is, of course, not possible to talk about these rights, either in ancient Rome or Medieval London, in a modern sense. First, because such individual rights were reserved to a very small segment of society, and, second, in the medieval times they were also founded on a concession from the ruling power (Periñán, 2012, p. 198).

The next big developments in the legal history of privacy are connected to the gradual emergence of the 'subject figure', the actor and the beneficiary of liberal democracy (Picard, 1999, p. 58), which can be seen as the first manifestations of the modern right to privacy. The first can be found in the adoption of the Post Office Act in 1660 in England, which committed the state to the provision of 'constant posts for the carriage of letters to all places' (Vincent, 2016, p. 46). This led to a high increase in the volume of correspondence and an increased expression of personal thoughts and emotions on paper, so that the transmission and receipt of the letter came to be seen as sustaining a personal relationship. Expectations of its confidentiality – expecting that the letter will be opened only by the addressee – thus increased (*ibid*., p. 48). Finally, in the Post Office Act of 1710 users were granted the confidentiality of correspondence, together with an enhanced defence of the threshold of the home to invasion by agents of the state (*ibid*., p. 51). The UK secretary of state, however, retained the power of issuing confidential warrants to open the mail of presumed enemies of the state,[105] leading to a two-tier approach to government surveillance that has continued with some modification to present day, particularly in the United Kingdom (*ibid*.).

104 See Darlow, B. (2003). History of defamation. Retrieved March 25, 2019, from https://englishlegalhistory.wordpress.com/2013/10/18/history-of-defamation/.

105 E.g. the famous Mazzini scandal in 1844, in which the Home Secretary, Sir James Graham, became the centre of a political scandal in 1844, when he was found to be opening the mail of Italian exiles in London at the behest of the Austrian government (Vincent, 2016).

In 18th century England, protection of the home (a sanctuary), expanded from the action in trespass in common law to include rules on search and seizure (Bradley, 1981, p. 464). This occurred in the famous 1763 *Entick v. Carrington* decision, which voided the legitimacy of general search warrants. Moreover, the Court conceptualized the protection afforded as going somewhat beyond the protection of property, submitting: '[T]hough the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass'[106]. This decision and further development led to a crystallisation of the idea of essential jurisdictional limits to the types of human activities that the state could legitimately regulate and prohibit by the end of the 18th century. There emerged a new, modern understanding of sovereignty, where the jurisdiction of the state was subject to fundamental limits, most notably of the limits to intrude into a human mind, one's home or into private papers. These limitations set forth a legally protected private sphere (as opposed to a public sphere), which still forms the foundations of the Western conception of the right to privacy (I discuss this in the next section).

The next relevant change in the law came in the 19th century with the emergence of libel laws and aimed at the press.[107] The English 1843 Libel Act was aimed at what was called 'the Paul Pry nuisance' (Vincent, 2015), offering rather limited protection from the press, which came to be seen as 'printed gossip.' English courts were, however, generally reluctant to extend the patchwork of judgments into anything resembling a general right of privacy distinct from the enjoyment of physical property. Instead, they upheld the freedom of the press to report in salacious detail on any domestic scandal that reached the public domain, especially as a consequence of the legal process itself (Vincent, 2016, p. 73). Finally, in 1890 Warren and Brandeis sought to establish a new legal right to privacy in the U.S. amidst the prevailing confusion of judgments and legislation and a growing concern about privacy. Their endeavour was partially based on the fact that the press ('the Paul Pry nuisance') was overstepping 'the bonds of propriety and decency' and the problem of print was being compounded by the new technology of cheap and instant photography. Despite the patchwork of cases and legal provisions presented above, it can be claimed that privacy was still

106 Entick v. Carrington Camden's judgement (1765), 19 State Trials 1045, pp. 391-397 (available at https://web2.uvcs.uvic.ca/courses/lawdemo/DOCS/ENTICARR.htm).

107 Similarly (although seemingly offering stronger protection) in France, the Statute relating to Press of 29 July 1881 (modified by the *Ordonnance* from 6 May 1944), which prohibits, in principle, the diffusion by the Press of any factual information, true or untrue, adversely affecting a person's honour or reputation (constituting the offence of defamation; Picard 1999, p. 54).

largely a social phenomenon (as discussed in Section 2.1.1) before the publishing of Warren and Brandeis' article, proclaiming the 'right to be let alone' (Vincent, 2016, p. 78). It is thus not surprising that Warren and Brandeis are often seen as the 'founders' of the right to privacy (e.g. Blok, 2002, p. 24; de Graaf, 1977, p. 13). This led to a surprisingly quick spread of the idea so that, as Allen and Rotenberg (2016, p. 35) put it: 'By the close of the nineteenth century the concept of a right to privacy had begun to garner adherents. It garnered even more adherents in the early years of the twentieth century, moving from the musings of a few visionary journalists, lawyers, and feminists into the hearts and minds of the general public.'

After World War II, privacy was translated from a set of relatively uncertain legal interests to a fundamental expectation at the end of the first half of the 20th century, primarily with the introduction into the Universal Declaration on Human Rights and the European Convention on Human Rights, resulting in a human right to privacy (I discuss this in Section 4.2.4). This development, however, did not lead to a single, comprehensive outcome. As Vincent (2016, p. 128) put it: '[A] co-ordinated programme of [secondary] legislation required a narrowing of ambition and a redefinition of the networks in need of protection.' The post-war translation of privacy into national law hence remained piecemeal, often specifying the home or the family as the main protection-worthy unit. Governments, however, retained wide powers in case of a perceived threat to national security, which were widely deployed during the global conflicts of the 20th century, and less overtly in response to peacetime tensions. This can be seen as a continuation of the practice of 'secrecy about secrecy' (*ibid*., p. 104), which (at least in England) began in the first half of the 19th century.[108] Once the scale and complexity of the internet became apparent, governments (and businesses) saw unprecedented possibilities of accessing the thoughts and opinions of their subjects (see e.g. Borgesius et al., 2018). In an era of international terrorism we are thus observing renewed enthusiasm for hidden surveillance of potential security threats (Kosta, 2017; Lyon, 2014).

108 The English national security surveillance programme (*GCHQ*), which took on its modern form in this period, was notable precisely for the almost complete absence of public authorization or oversight. Ever since the 1844 Mazzini scandal, no new legislative basis had been created either for the subsequent growth of postal espionage or for newly emerging technologies such as the telephone, which had been subject to interception since its introduction. The position was and remains, at least in the UK, that surveillance of communication, if not formally legal, is at least not contrary to any known statute (the Intelligence and Security Committee's Privacy and Security report of March 2015; Vincent, 2016).

Whereas the legal concept and right to privacy remained rather unclear and piecemeal, the concept of data protection (regulating the processing of personal data), offered a more manageable field of concerted action, which led to a new wave of legislation across the developed world. With the emergence of computers and computerised databases in the 1960s, states began to use these increasingly sophisticated technologies for a wide array of purposes: the census, banking, taxation, credit-rating, criminal records, the railways and national insurance. Although this use was still in its infancy, it resulted in severe criticism of the perceived potential (rather than actual use) of these new technologies. The mid-1960s thus bring the beginning of the 'end of privacy' proclamations or panics (alongside sensible reports, e.g. *Records, computers and the rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973). This initial phase of apocalyptic predictions was translated into a growing body of laws, including the regulation of wiretapping and covert observation by law enforcement. The focus of subsequent legal protection in the 1970s (and continuing to this day), however, was on 'informational privacy', beginning with the first national data protection law in Sweden in 1973, which was a response to fears about the computerised census. This agenda of legislative reform, however, belonged primarily to the realm of data protection, which falls outside the scope of this dissertation.

4.2 Key contemporary perspectives on the right to privacy

Based on the above – admittedly non-exhaustive – historical account, the roots and first examples of the right to privacy can be identified: protection of one's home, communications, personality rights (e.g. the right to one's name, reputation, honour), and the limitations imposed on law enforcement (e.g. search and seizure) and the press. Privacy as a legal concept thus surfaced historically associated either with personal freedom (defamation and libel laws, secrecy of communications) or as an element of property law (protection of the home), particularly in common-law jurisdictions (González Fuster, 2014, p. 24). These emanations (or certain combinations of them) can be and have been considered as the traditional core of the right to privacy (e.g. Picard, 1999, pp. 49–50; van der Sloot, 2015) and still form the basis of the modern conceptualisation(s) of the right to privacy. Before I focus on the more recent developments (shifts and expansions) of the right to privacy in Europe, I will zoom into these more traditional conceptualisations and manifestations of privacy law.

4.2.1 The 'original' right to privacy: Warren and Brandeis' right to be let alone and Prosser's privacy torts

The search for origins of privacy as a legal institution seems to come easily in Anglo-American legal writing. Warren and Brandeis' famous *The right to privacy* article (1890), which they wrote as a response to the prying and gossip of the *yellow* press, is seen as

the origin of privacy as a legal value not only in the U.S. but in the West in general (Blok, 2002, p. 24; Strömholm, 1967, p. 25). Although the authors are indeed the first to coin a legal concept of the right to privacy, thus giving it its most widespread name, they relied on already existing ideas of legal interests in private relationships free from government interference, both from U.S. jurisprudence as well as from Europe.

Specifically, they were inspired by 19th century U.S. jurisprudence that recognised legal interests in private relationships free from government interference already prior to the article (most notably, Prince Albert v. Strange [1849] 1 McN & G 25; Allen & Rotenberg, 2016, p. 17).[109] Furthermore, they built their right to privacy partially based on English case law of the first half of the 19th century and partially on a French 'Law of the press' (*Loi relative à la presse*) from 1868, which prohibited the publication of facts related to the private life of individuals (unless they were already public or were published with their consent) (Brandeis & Warren, 1890, p. 214). Based on these conceptual roots, Warren and Brandeis mapped out a new 'invasion of privacy' tort, calling it 'a right to privacy' and 'a right to be let alone', a term which they borrowed from the prominent nineteenth century tort scholar Thomas Cooley (Allen & Rotenberg, 2016, pp. 22–23). This 'general right of the individual to be let alone' offered protection to thoughts, sentiments, and emotions, based on the principle of inviolate personality, receiving the same protection regardless of the type of expression (in writing, in conduct, in conversation, in attitudes, or in facial expression) (Brandeis & Warren, 1890, pp. 205–206). The right to be let alone constitutes a 'right not merely to prevent inaccurate portrayal of private life, but to prevent its being depicted at all' (*ibid*., 218). Their article was so influential already at the time when it was written that 'the American courts installed the right to privacy in the common law within a single generation' (Allen & Rotenberg, 2016, p. 23). Already in 1891, the U.S. Supreme Court in the *Union Pacific Railway Company v. Botsford* case endorsed Warren and Brandeis' idea that a 'right to be let alone' is embodied in the common law. It only took a few years' time for the tort to take off in state courts (*ibid*., p. 39).

In 1960, further work on privacy torts was done by Dean Prosser, whose article on privacy torts (1960) has been called 'the most successful attempt to analyse the American concept of privacy' (Strömholm, 1967, p. 46). Prosser provided a systematisation of the invasion of privacy tort, which essentially became recognised by the law (Richards, 2011). He analysed a half century of tort cases that had adopted the Warren and Brandeis theory and concluded that the invasions into one's privacy

109 Albeit sometimes in order to legitimise slave and wife beating, as feminist critique has pointed out (Allen & Rotenberg, 2016, p. 17).

have no common conceptual core, except that they interfere with the right to be let alone (Prosser, 1960, p. 389). He thus split up the invasion of privacy tort, organising it into four categories: (1) intrusion upon seclusion or solitude, or into one's personal affairs; (2) public disclosure of embarrassing facts; (3) publicity that places one into false light in the public opinion; and (4) appropriation of one's name or likeness for another's personal or pecuniary advantage. The first kind of intrusion seeks to fill 'the gaps left by trespass, nuisance, the intentional infliction of mental distress, and whatever remedies there may be for the invasion of constitutional rights' and protects a mental interest (*ibid*., p. 392). The second and third kind protect one's reputation and extend the established torts of libel, slander and defamation. The fourth protects a mostly proprietary interest, whether it is classified a 'property' or not, since it has value and can be licensed. This splintering of the privacy tort has been described as a 'momentous move', which proved incredibly persuasive for the remaining wavering state courts and legislatures, which up until then saw the privacy tort as a contested and largely undefined right (Schwartz & Peifer, 2010, p. 1940).

Although Warren and Brandeis (with further work from Prosser) can indeed be seen as the intellectual founders of the right to privacy in the U.S., it does not make sense to limit the broader concept of the rights to privacy (or privacy law) to this first attempt (no matter how marvellous it indeed was). First, this right to privacy offers protection only via private law. Second, the four types of tort actions that are available are still quite limited, especially in comparison with the far more open-ended protection by a similar legal tool common in continental Europe – personality rights (discussed in the following Section). Whereas in continental Europe, personality rights (including the right to privacy) are protected on the constitutional as well as private law level, constitutional privacy protection in the U.S. is based on a different legal source, particularly the Fourth Amendment.[110] I examine these other emanations of privacy law, particularly in Europe, below.

4.2.2 The right to privacy as a personality right

Although some authors dispute the connection between personality rights and the right to privacy (e.g. van der Sloot, 2015), many other, particularly European scholars, have claimed that personality is so closely related to privacy, that the two are sometimes confused with each other (Blok, 2002, p. 10, see ref. 4; Strömholm, 1967). According to Strömholm (1967, p. 21), the legal concept of the right of personality is a concept akin to privacy and a major reference for the right to privacy in continental

110 The Fourth Amendment falls out of the scope of this dissertation.

Europe.[111] In fact, the German Constitutional Court (*Bundesverfassungsgericht*) traced the developments of a general 'right to informational self-determination' (*informationelle Selbstbestimmung*) to the fundamental right to the 'free development of one's personality' protected by Article 2.1 of the German Constitution (*Grundgesetz*) (Rouvroy & Poullet, 2009, p. 49).[112] As mentioned above, Warren and Brandeis (Brandeis & Warren, 1890, p. 195; following Cooley) also based their right to privacy on inviolate personality, rather than on the principle of property, which traditionally played a bigger role in privacy law in the U.S. (Blok, 2002, p. 30). As such, personal interests form the object – at least to a certain extent – of the continental European as well as Anglo-American right to privacy.

The concept of personality rights is old and can be found, at least to a certain degree, already in Roman law (see Section 4.1 on *actio iniuriarum*) but developed more fully at the end of the 19th century, particularly in Germany and France.[113] It is connected to ideas of classical natural law and its notion of innate, inalienable human rights, which include various rights relating to personality (Hubmann, 1967, p. 85; Neethling, 2005, p. 210). Today the idea of personality rights as a separate group of private rights is firmly established in continental Europe (and in certain other places around the world, particularly countries that were colonised by European states). Personality rights have thus been described as rights recognising the person as a physical and spiritual-moral being that guarantee one the enjoyment of one's own existence (Neethling, 2005, p. 210).

Although there is no exhaustive list of personality rights in most countries (they are often described as 'by nature inexhaustible'), they commonly include: a person's exclusive right to one's name and the actions pertaining thereto, the right to one's own likeness and the rights to honour and liberty, including the liberty to organise

111 E.g. France, Germany, Italy, Greece, Switzerland, Austria, Poland, Hungary, Yugoslavia etc. This does not hold for Scandinavian countries, though, where the notion of 'rights of the personality' never gained much ground.

112 It did this in its famous 1983 decision with which it established the general right to informational self-determination; BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 ('Volkszählungsurteil').

113 The Roman *actio iniuriarum* was often invoked in German legal writing before the adoption of the German Civil Code (*Bürgerliches Gesetzbuch*; BGB) and the same is true for Dutch law (Strömholm, 1967, p. 41).

one's private life (Strömholm, 1967, pp. 49–50).[114] Furthermore, personality rights also include rights inherent to the person as a member of a family (e.g. marital status) and rights that are attached to the status of a citizen (e.g. nationality, right to vote; *ibid*., p. 50). As these (types of) rights are of considerable significance for individuals, most personality rights have been entrenched as fundamental and human rights.

The classification of privacy as a personality right says something about the meaning of privacy. First, if the right to privacy is a personality right, privacy is understood as being inalienable (cf. Rouvroy & Poullet, 2009, p. 52). Indeed, the transfer of one's private sphere to another is rather unimaginable. This also means that the right to privacy is a personal right, meaning that it can only be asserted by the person whose privacy has been invaded (although there are certain effects of personality rights after death as well and, moreover, personality rights of children and those with intellectual disabilities are enacted by others on behalf of them). Second, the right to privacy is not concerned with providing material gain to the individual, since the value of personality rights is found in non-monetary interests (the harm caused by its infringement is thus often immaterial). The right to privacy, stemming from the theory of personality rights, namely has the goal of providing the individual the opportunity for the 'enjoyment of one's existence'. Third, connected to this fundamental role of personality rights, most are protected by private law as well as constitutional law. It thus follows that the right to privacy as a personality right should be protected both on a constitutional and civil law level. Finally, as personality rights in Civil Codes (and national constitutions) are often incredibly broad, including very diverse interests from the secrecy of confidential letters, the right to a person's name, and unwarranted publication of a person's image, this can pose an obstacle to the elaboration of a coherent legal theory of both personality rights as well as the right to privacy. Most French theories of privacy of the early 20th century, for example, stated that the notion of 'right to the personality' (*droits de la personnalité*) is far wider than that of privacy in

114 The protection of private life in the German legal system is a part of the general personality right (F. de Graaf, 1977, p. 30). In the beginning of the 1950s, Hubmann analysed the right of individuality (*Recht auf Individualität*) as the protection of three distinct spheres: (1) the *sphere of individuality*, which comprises a person's name, trade name and honour; (2) the *private sphere*, which refers to the protection from publication of one's likeness or image, including 'the portrait of one's life' and one's character (*Lebensbild* and *Charakterbild*), as they can be read out of words, acts, handwriting and other elements capable of interpretation by scientific methods; and (3) the *sphere of intimacy*, which protects not only against publication, but also against any act by which a third party can obtain knowledge about things as confidential notes and letters (Strömholm, 1967, p. 56). This classification has been adopted by many other authors within and beyond Germany as well as the German Supreme Court (*Bundesgerichtshof*; BGH) already at the end of the 1950s (e.g. BGH, 20 May 1958, in GRUR 1958, p. 615).

the 'original' U.S. context (Strömholm, 1967, p. 49). The conceptualisation of privacy as a personality right is, thus, said to be not only much wider but also much vaguer than the concept of privacy in a strict or 'original' way, as conceptualised in U.S. law (*ibid.*, p. 43). This perspective is particularly relevant for the discussion of the right to respect for private life in Article 8 ECHR, as it has been interpreted by the European Court of Human Rights (ECtHR), which I examine in Chapter 6.

4.2.3 The private spheres theory

Following a small succession of influential decisions of the German Federal Constitutional Court (*Bundesverfassungsgericht*; BVerfG),[115] German legal theory conceptualised the private realm (and consequently the right to privacy) as a series of concentric circles moving from the inner self outwards to include family, friends, civil society, larger groups and, finally, the state. Different degrees of protection are offered to these different levels (circles) of the private sphere.

This theory became very influential beyond Germany, leading to several more or less different conceptualisations of such concentric circles emerged both in theory (e.g. Alexy, 2010; Picard, 1999, p. 60; Richardson, 2016, p. 91; Rössler, 2005; Roßnagel & Geminn, 2015) and in national privacy case law, both in civil law as well as in common law systems. Although these conceptualisations do differ, their differences are rather small and do not have much bearing for the purpose of this debate.

Alexy (2010, p. 237), for instance, distinguishes three main spheres of decreasing intensity of protection: (1) the innermost sphere, which refers to the innermost field of privacy and is understood as an inviolable sphere of intimacy – 'the final inviolable field of human freedom'; (2) the broader sphere of privacy, which includes private life to the extent that it is not already covered by the innermost sphere; and (3) the social sphere, which includes everything which is not already covered by the private sphere. Similarly, Picard (1999, p. 60) describes the inner most circle as confined to what the subject possesses as the most intimate of his person, that is her thoughts, beliefs and values. The second circle, a much broader ring, encompasses the external characteristics of the person and her intimate social life, which involves other people, at first instance family and friends. The third and last circle, the limits of which are

115 See e.g. BVerfGE 6, 32; BVerfGE 27, 1; BVerfGE 27, 344; BVerfGE 32, 373; BVerfGE 43, 238; for more see (Rohlf, 1980, p. 70).

least clear, is made of 'external projections of private life' (*ibid*., p. 60).[116] These include relationships, which the person, in order to lead her own personal life of the first and second circle, needs to have with persons beyond these spheres and might require presence in public space.

According to Alexy (2010, p. 237) the first sphere is considered to be inviolable, since in that sphere the individual is considered as not affecting others by her existence or behaviour, thus not disturbing the personal sphere of others or the requirements of life in community (generally in line with the 'harm principle'; Feinberg, 1984).[117] Accordingly, the other two spheres are offered increasingly less protection. Contrary to Alexy, Picard (1999, p. 60) posits that the second circle deserves the strictest protection, as this sphere proves more permeable to intrusion. Furthermore, the third circle also deserves protection of privacy, although admittedly to a lesser degree – only to the extent of the 'external means of private life' (*ibid*., p. 60):

> 'Now, [the person's] presence in [public] places, the company which he keeps, his image, which all belong to his private life, are displayed outside the second circle. None the less privacy here does not disappear, at least not thoroughly. In this third circle, we are faced with elements of private life carried out in public which, too, deserve the protection of privacy.'

This external dimension implies that others may see and know all that is visible and knowable, however, they should refrain from divulging it to a wider public unless the person accepts (or tolerates) this. According to Picard (*ibid*., p. 61), this aspect of the right to privacy is, however, not well thought out in practice – 'judicial decisions do not usually refer to this distinction, except where the judges seek a formal justification in order to refuse privacy in borderline cases.'

Moreover, despite its instinctive attractiveness, the boundaries of the spheres are very difficult to determine, so that the circles/spheres theory has been criticised as 'an

116 Rössler (2005) offers a very similar account of the circles as Picard but calls this theory the 'onion model' (*Zwiebelmodelle*), distinguishing the following layers: 1. the sphere of personal (bodily) intimacy and privacy (such as a private diary) compared to which all other layers are 'public'; 2. the second layer is the classical private area, namely family or other intimate relations; 3. the last layer is the societal, or state layer, which forms the outer edge of the public sphere.

117 This has been criticised especially by feminist scholars (MacKinnon, 1987). Their critique primarily targets the notion that there is an inviolable intimate core that does not affect others. Based on this reasoning, the law has until recently allowed for the abuse and subordination of women by men within the 'privacy' of one's home.

extremely crude description', a rough classification of the nature of interests involved (Alexy, 2010, p. 239). Although the doctrine can be a useful complement to the more mechanical study of different objects of protection, this approach, as Strömholm (1967, p. 75) argued already in the late 1960s, should not be more than an analytical instrument and should not be treated as a fixed rule. Nevertheless, as Picard pointed out, national courts still fondly use a simplified type of classification when dealing with privacy cases, however, resulting in an exclusion of the private aspects of our lives in public (cf. Nissenbaum, 1998).

4.2.4 The human and fundamental right to privacy or private life

The recognition of right to privacy as a unitary right at a constitutional level is a rather late phenomenon. As discussed above, it was preceded by specific provisions on the inviolability of the home and the secrecy of communications (also González Fuster, 2014, p. 23). A general right to privacy emerged later, sometimes subsuming previous specific provisions, sometimes supplementing these. Particularly in Europe, supranational law – most notably the European Convention on Human Rights (ECHR) – supplied fundamental points of reference for discussion on the right to privacy and still plays a leading role in determining the meaning and scope of the rights to privacy.

After the Second World War, the right to privacy (along with many other rights) finally came to be elevated to the status of a human right. The first international law document that positioned the right to privacy as a human right was the Universal Declaration of Human Rights (UDHR or Declaration), which was adopted by the General Assembly of the United Nations in 1948. Article 12 of the UDHR states:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

This article was based on national constitutional provisions (from the entire spectrum of political persuasions around the world), which declared the inviolability of the home or secrecy of communication. Unlike most articles in the Declaration, however, Article 12 on privacy is stated in a negative mode of expression, implying that everyone has these inherent rights because they are said to have the right to be protected against interferences in this realm of privacy (Morsink, 2000, p. 134). According to Morsink (2000, p. 135), one of the difficulties with phrasing in regard to Article 12 had to do

with the disparate character of the rights in question[118] and the practical issue of how to capture them in one good sentence. The provision was drafted in the way it was, partially because the language of inviolability did not fit all of the protected interests equally well and because it implied too strong (absolute) protection.[119]

Although the Declaration did not include any machinery for its own implementation, it has been the foundation of much of the post-1945 codification of human rights, so that 'the international legal system is replete with global and regional treaties based in large measure, on the Declaration' (Morsink, 2000, p. xi). Most importantly, the Declaration served as the foundation for the drafting of the European Convention on Human Rights (Blackburn, 2001, p. 9), which can be described as the most important European human rights instrument ever (González Fuster, 2014, p. 81).

While Article 8(1) is derived from Article 12 of the Declaration, the progenitor of Article 8(2) is Article 29(2) – a general limitation applying to all of the rights and freedoms in the UDHR.[120] The ECHR, however, introduced several changes. The most notable difference lies in the terminology – rather than referring to 'privacy', Article 8 refers to 'private life'. Schabas (2017, p. p. 369) posits that this is a 'difference, which does not seem to have any legal consequences, [and] may be related to the important role of the French language in the drafting of the European Convention, "private life" being a somewhat awkward rendering of 'vie privée.'

Article 8 ECHR is divided into four categories: private life, family life, home, and correspondence. The jurisprudence concerning the category of private life is overwhelming by comparison with the relatively few cases relating to the home and correspondence (Schabas, 2017, p. 336). In fact, there is no neat dividing line between these categories and several cases examine them together (either both private life and the home or both private life and correspondence). Furthermore, the range of rights protected under the umbrella of 'private life' itself is very wide. Article 8 has proven to be one of the richest areas of legal development by the Court in recent years (*ibid*., p. 366). Cases relating to the general right of respect for private life range from health

118 The draft provision initially included ‚personal property' but that was later dropped as it was covered by what became Article 17 (Morsink, 2000, p. 139).

119 'Inviolability' was commonly used in relation to the home, 'secrecy' or 'privacy' in regard to correspondence and ‚respect of' in the context of honour and reputations (Morsink, 2000, p. 136).

120 Article 29(2) UDHR states: 'In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.'

and medical care, employment and professional activities, sexual activity, dying, honour and reputation, to personal autonomy and identity, private data, physical and psychological integrity, and even environment cases (ibid., pp. 369-88). As Rainey, Wicks and Ovey (2017, p. 400) put it:

> 'It was suggested some years ago [by Velu 1973] that the Convention protects the individual, under this head, against attacks on physical or mental integrity or moral or intellectual freedom, attacks on honour and reputation, the use of a person's name, identity, or likeness, being spied upon, watched, or harassed, and the disclosure of information protected by the duty of professional secrecy. This has proven to be the case.'

Moreover, the right to respect for private life is also considered not only as a negative obligation (in the sense that governments need to abstain from certain acts) but also as a positive obligation, according to which governments are obliged to perform certain actions so that this right is protected. According to Loucaides (1990, p. 178), the right to respect for private life has developed in 'an impressive and progressive manner and has abandoned certain of its earlier and more conservative jurisprudence.' In view of the established approach that the Convention is a 'living instrument', whose interpretation may develop through the years, we may come to see new rights derived from the notion of 'private life' whenever this would be required by the conditions of social life (*ibid*.). As I analyse the case law of Article 8 ECHR in relation to protection of privacy in public space in Chapter 6, I will leave the discussion here at this.

5. CONCLUSION

Studying privacy is humbling, as Solove (2008, p. ix) appropriately put it. It is difficult to find one's way around the complexity, philosophical richness, contemporary relevance and an 'overdose' of literature, especially for legal scholars. In order to gain a sufficiently good grasp on this complex notion, I have offered in this Chapter a broad overview of the conceptualisations of privacy – both as a theoretical and a legal concept. As already explained in the Introduction, I have intentionally avoided the focus on informational privacy. I have done so because this type of privacy has been dominating the fields of privacy law and literature ever since the 1960s. As Jean Cohen (1997, p. 140) put it, the debates are over the extent, rather than the very idea, of informational privacy.

The above examination of privacy theory (including legal theory) is rich in insights. In this conclusion, I will limit myself to pointing out three insights that bear particular

value in relation to the focus of this dissertation, that is privacy in the context of surveillance of public space within smart cities and living labs.

The first is that privacy as a theoretical and linguistic concept has been evolving, both in the sense of changing in focus but also widening, ever since it emerged. Consequently, the many aspects and characteristics of the concept of privacy, its elusiveness, are not something that needs to be (or indeed should be) discarded but is – or at least can be – its strength. In this sense, one can follow Mulligan, Koopman and Doty (2016, p. 3; following Gallie 1956) and call privacy 'an essentially contested concept', where disputes about its core are both paramount and central to the concept itself (as, for instance, with 'democracy', 'art' or 'freedom'; Gallie, 1956, p. 149). Taking this elusiveness (or essential contestedness) as a positive feature, we can better recognise privacy as a means for responding to problems created by technology and societal change. As Gallie (1956, p. 184) put it, essential contests are an 'actual inchoate condition of growth'. Such a perspective on privacy seems particularly suitable for privacy in public space in the context of surveillance within smart cities and living labs. If privacy in public did not exist as a real problem in the recent past, simply because individuals achieved a generally satisfactory level of privacy there through social mechanisms, new practices and technologies of surveillance have changed this (Nissenbaum, 1998). Moreover, if a binary conception of private *versus* public (space, activity or data) has served our privacy needs well enough until now, this might no longer be the case.

This is connected to the second point, according to which privacy theory is increasingly emphasising the value of privacy not only for the individual but for society more broadly, particularly from the 1990s onwards. This holds particularly in relation to the forming and maintaining social relationships (both intimate or primary as well as secondary relationships) but also in regard to democracy and values of pluralism. In this latter sense, privacy has been seen not only as a value in itself but also as a value that is crucial in relation to other fundamental rights and freedoms, such as freedom of expression and freedom of assembly and association. Privacy is thus a 'part of a package of intertwined fundamental rights' that guarantee not only our individual but also social and political emancipation (Gutwirth, 2002, p. 45). Or, as Koops (2018) put it, privacy is an infrastructural condition. It is an important presupposition for autonomy, self-development, and the other values that privacy contributes to; and it is because privacy can serve many other values that it is also a value in itself (ibid., p. 621). This is particularly valuable in regard to the relationship between surveillance and privacy, which is discussed in relation to the *Stratumseind Living Lab* in the Chapter 5. There is, namely, a particular disconnect between these two concepts. Surveillance

studies scholars commonly employ a very narrow conception of privacy, often limited to a simplistic perception of the right to protection of personal data, positing that the risks of surveillance go much beyond risks for privacy. As such, their argument goes that privacy is not the sole or the best means to regulate surveillance (e.g. Lyon, 2001). However, in view of the infrastructural character of privacy (both as a concept as well as a right), this claim can and should be questioned.

Finally, this allows me to settle on a definition of the concept of privacy, which I will be employing throughout the rest of the dissertation. Following Julie Cohen (who nicely relates this definition to several accounts of privacy as described above; 2017, p. 458), I understand the condition of privacy as 'breathing room for socially situated subjects to engage in the processes of boundary management through which they define and redefine themselves as subjects.' As such, rights to privacy need to be understood in a similarly broad sense as 'the sociotechnical conditions that make condition of privacy possible' (*ibid*.). In other words, privacy law preserves – indeed, should preserve – possibilities of achieving privacy (similarly Austin, 2019). As the concept of privacy is not rooted or limited to private space, this applies to public space as well. Indeed, a similarly broad conception of privacy (while not without its critics) seems to be found in the interpretation of Article 8 by the ECtHR, which I examine in Chapter 6.

In this dissertation I have thus far examined three foundational notions, as I have referred to them: smart cities and living labs (which I examined together due to their close connection), surveillance and privacy. There is, however, another foundational notion in the context of privacy in public space that requires exploration – public space. I engage with this complex concept, particularly through the fields of human geography and political theory, in the next Chapter.

4

PUBLIC SPACE
Shades of privateness and publicness*

* This Chapter uses parts of text from a co-authored chapter, Conceptualizing space and place (Koops & Galič, 2017). The co-author has granted me permission for this.

1. INTRODUCTION

Especially since the 1990s, the *make-up* of public space has been changing significantly. Public space has been becoming more sentient, empowered by the proliferation and increasing sophistication of embedded sensors and other surveillance technologies, including smart CCTV, wifi, cellular networks, wireless mesh technologies, sound sensors, and automatic license plate readers (Timan, Newell, et al., 2017a, p. 2). Such surveillance is said to be transforming the public-private divide and 'polluting our privacy' in public space, as Froomkin (2017, p. 184) put it. While law continues to assume a more-or-less fixed and clear-cut distinction between private space – with a strong level of privacy protection – and public space – where there is hardly any protection of privacy –, lawyers should learn from the insights of geographers and other fields of academic research relating to space and place in order to better determine the value and a desired level of privacy protection in public spaces (Koops & Galič, 2017, p. 20). However, privacy is still too often defined and studied in a de-contextual and abstract manner, also (or especially) by legal scholars. This is so despite a clear indication that it should be studied locally and in context by many scholars (see contributions in Newell, Timan, & Koops, 2019; Timan, Newell, & Koops, 2017b). This need to study privacy in context, holds particularly true for the disputed and problematic notion of privacy in public space, where an essential part of the context is found in the concept of 'public space', with its own physical, social and cultural peculiarities and logic. Before I analyse the particular types and characteristics of surveillance in the *SLL* and, particularly, the privacy-related risks stemming from them (see Chapter 5), the concept of public space needs to be examined in more detail. This is the general aim of this Chapter in which I rely primarily on key insights from human geography[122] but also from literature on space and place from other fields (including psychology) that are relevant for the debate on privacy in public space. This is essential in order to determine what privacy and the right to privacy in public space is and is not, can or should (not) be.

The concept of space has become very topical in the recent past, so much so, that our historical moment has been called the 'epoch of space' (Foucault, 1986, p. 22). On the one hand, space has been described as 'the everywhere of modern thought' (Crang & Thrift, 2000, p. 1), as a broad range of disciplines, including sociology, philosophy and cultural studies, have experienced a 'spatial turn' in the later 20th century (Massey, 1992; Soja, 1996; Warf & Arias, 2009). This spatialisation of social theory is said to

122 Urban geography, which was the main source of literature in Chapter 1, is a strand within the broader sub-discipline of human geography.

be based on the need for a more enhanced appreciation and even prioritisation of how space matters to our understanding of society (Featherstone, Lash, & Robertson, 1995, p. 1; Soja, 1996, p. 46). In the last fifty years, there have thus emerged many theoretical discussions concerning the importance of space and place in shaping cultural, social, economic and political life. On the other hand, geography experienced a 'cultural turn' of its own as it began to engage with social theory, drawing from authors such as Foucault, Bauman, Lefèbvre, Habermas, and Arendt. It should come as no surprise then that the topic of space, including public space, is highly complex and multi-dimensional. Moreover, the emphasis on the concept of space should not be overlooked in fields of law and privacy theory. In order to understand what public space *is* and *does*, and how this particular spatial context influences our experience and expectations of privacy when we move around in public space (Koops & Galič, 2017, p. 19), we – lawyers and privacy theorists – need a deeper understanding of (public) space and place.

The central focus of this Chapter is on physical urban space of Western societies, with its particular political, social and psychological significance. As the aim of this Chapter is to unveil various aspects of urban public space that are particularly relevant for my conceptualisation of privacy in public space, I examine public space from multiple perspectives. First, I employ a socio-spatial perspective, asking questions such as 'what are public space and place?' or, rather, 'how are public space and place made?' Second, I examine public space from a political perspective, engaging with theory on public and private spheres and, moreover, on the public-private distinction. Third, I analyse contemporary power shifts in public space, focusing on issues of privatisation and securitisation of public space. In connection to these issues of power, I briefly review how law deals with public space, focusing on public nuisance laws and 'security zones'. Finally, in the last part, I delve into the connection between space and identity-building, especially in light of recent socio-technological developments such as time-space compression and de-territorialisation. I conclude this Chapter with a succinct recapitulation of the key insights learned from the examination of public space and the public sphere, and their implications for privacy in public space.

2. THE MAKING OF SPACE AND PLACE

While 'public space' is a term commonly used in everyday life with an intuitive and seemingly straightforward understanding of its meaning, that is not the case, when the concept is examined more closely. In fact, there is a rich literature on the matter, discussing foundational concepts such as space and place. Thinking about space has

roots in philosophy, most notably in the thought of Descartes, Leibniz and Newton (Tally, 2013, pp. 27–28). Newton, for example, saw space as an independent, three-dimensional, infinite container of matter, which is a conception that still dominates lay thought on space. Somewhat similarly, Descartes saw space as intrinsically related to the dimensionality of masses (or bodies) in space, which is reflected in the notion of Cartesian space. On the contrary, Leibniz posited that space is fundamentally relational. As such, space does not exist in itself, rather, it is the relation between bodies. In the context of these philosophical ideas on space and developments of the 'scientific revolution', geography emerged as a distinct discipline in the 18th century. At least until the 1950s, the dominant strand of geography was that of 'physical geography' studying the natural environment, which saw physical space in a Newtonian way as an 'empty and neutral container', a backdrop against which human behaviour is played out. Space was thus understood as straightforwardly empirical, objective and mappable, where phenomena were seen to pre-exist their location in space. In the 1970s, however, various approaches in geography arose that employed a more Leibnizian view of space. These approaches can be termed 'critical geography' and include behaviourist, human, structural or 'radical' and post-structural approaches to geography (Koops & Galič, 2017, pp. 21–22). For the purpose of analysing privacy in public space, this Chapter will focus on human geography, as this strand of research approaches geography through the lens of human experience, studying people and their condition in relation to space and place.

Human geographers debate the nature of space and place and ask themselves, 'how space *becomes*?' instead of 'what *is* space?', as physical geographers do. They see space as socially co-produced, rather than as a common-sense external background to human and social action (Lefèbvre, 1991; Thrift, 2003). As such, spaces are subtly evolving layers of context and practices that fold together people and things and actively shape social relations. Space is, thus, a product as well as a medium. As Kitchin and Dodge (2011, p. 65; emphasis in original) put it:

> 'Social relations do not operate independently of space or simply at a location, rather space is an *active* constitutive element in the production of social relations, communal formations, political organization, and personal regulation. In other words, the social is inherently temporal *and* spatial.'

This means that space is in a continuous state of becoming/being made through emergent patterns of use (Berman, 2006), where old forms of space disappear and

new ones emerge (Neal, 2010). The function of space, therefore, alters with time.[123] This perspective on space further leads to another common distinction that is relevant for the discussion of privacy in public space – the one between space and place.

2.1 Space and place

The use of terms 'space' and 'place' is often interchangeable, both in popular speech as well as in many disciplines not informed by geographic theory, including law. While the conceptual debate is ongoing, there is a rough consensus that space is a more abstract concept than place (Cresswell, 2015, p. 15). Space is associated with Cartesian and Newtonian conceptions of the physical world, seen as a given container, in which matter is located somewhere along three dimensions (Hubbard & Kitchin, 2011, p. 4). Place, on the other hand, is seen as socially co-produced and not given. This means that, when spaces come to function in specific ways, with distinct characteristics and meaning in a particular context, *space becomes place* (Koops & Galič, 2017, p. 23). Place can hence be defined as 'meaningful location' (Altman & Zube, 1989, p. 2; Cresswell, 2015, p. 12). In line with this definition, Tuan (2001, p. 179) has shown that the concepts of space and place can be correlated with movement and stability: a space can become a place when we stand still and observe. Places are, therefore, spaces we come to know and value. As such, places form the basic condition of life and are particularly relevant for identity-building (see Section 5.1). From the security and stability of place we can become aware of the openness, potentiality and threat of space, and *vice versa*. The ideal *place* then is often seen in the home, the archetypal private space – for many, the most meaningful, valued, stable and safe space a person can inhabit. This connects to the existentialist idea of 'being-in-the-world', which implies the process of dwelling, involving a continuity between a person and a place, seen as fundamental to human existence (Heidegger, 1971).

In contrast, public space can be seen as the ideal *space*, a site of openness, potentiality, of the unknown and the dangerous – a site of all sorts of activities, the presence of strangers and of movement (for example, when we are commuting between various more or less private places). However, in between these 'extremes' lies a gradation of in-between spaces or places, where transformations from one to another occur more commonly and quickly. When a public *space* acquires a sense of stability and meaning, particularly when it is used as a *place* for politics, sociability or personal memory and

123 Of course, this does not happen in a vacuum – rather, the use of space is negotiated and contested between individuals and groups, and increasingly affected by technological developments (Kitchin & Dodge, 2011). This will be examined in more detail in Section 4 on contemporary power shifts in public space.

meaning, it can become a public *place*. This process can then reverse and a public place reverts (back) to a public space, as the space ceases to be used for a particular political or social goal, for instance when it becomes too run down to serve as a space of social gathering, or as a previous space of sociability loses personal meaning when it is torn down or repurposed in a completely different way (for instance, when the cinema to which one went as a teenager is torn down and a new residential building is erected). Certain recent socio-technological developments also play an important part in this; for instance, technological mediation of communication can pull a place apart, making it a different type of place or turning it into a space (DeLanda, 2006, p. 12; see Section 5.2). An example of this can be seen in online shopping, which makes the venturing into a physical shop in public space (sometimes on a different continent) completely unnecessary. But the process of transformation can then revert again (as can be seen, for example, from the emergence of physical Amazon stores).[124]

Place and space are, thus, not mutually exclusive concepts, rather they form a spectrum, linking experience (place) to abstraction (space) (Cresswell, 2015, p. 37). In fact, space and place are highly related concepts constituting each other: a place takes meaning from the spaces outside it, and spaces are relevant to the places they surround (*ibid*., p. 48). They thus require and depend on each other in order to exist. This mirrors the relationship between the public and the private sphere, which can also be seen as interdependent spheres existing on a continuum (see Section 3.3). This is important for the debate on privacy in public because it allows us to distinguish a double meaning of the public: that of public *space*, representing the openness and potentiality of access and use (especially for the purpose of political participation), and that of public *place*, connected to identity-development and representing particular meanings for particular persons, groups and uses. Both of these have value in relation to privacy in public space, as I will show throughout this dissertation.

3. PUBLIC AND PRIVATE: A POLITICAL AND SOCIAL PERSPECTIVE

The division of social life into a public and a private realm or sphere – represented in the public-private distinction – is a cornerstone of liberal politics and liberal democratic theory. It serves as a point of entry into many key issues of social and political analysis, or moral and political debate, and of the ordering of everyday life

124 See Amazon physical retail locations. (n.d.). Retrieved March 21, 2019, from https://www.amazon.com/find-your-store/b/?node=17608448011.

(Parkinson, 2012, p. 50; Weintraub, 1997, p. 1). Bobbio (1989, p. 1) called it one of the 'grand dichotomies' of Western thought, seeing it as a binary (in the sense of exclusionary) opposition that is used to subsume a wide range of other important distinctions in an attempt to dichotomize the social universe in a comprehensive and sharply demarcated way. This distinction, however, is not clear-cut at all. In fact, the question of precisely where the boundary between public and private should lie is a matter of intense debate (see Section 3.3). Some, especially feminist, scholars have even argued that the distinction is becoming so blurred that it should be dismissed (Gibson-Graham, 2006; G. Rose, 1993). Nevertheless, the public-private distinction has proven compelling and enduring, and I will engage with it in this section.

The private and the public are thus contested realms that are heavily debated in various disciplines, including geography, political theory and feminist studies. Scholars in these fields often argue that we should be weary of too strict binary distinctions (along the lines of 'East is East, and West is West, and never the twain shall meet', as Rudyard Kipling famously put it), as they have an artificial and distorting effect. While binary distinctions may indeed be a useful analytic procedure, 'their usefulness does not guarantee that existence divides like that' (Douglas, 1978, p. 161; quoted in Weintraub, 1997, p. 1). Furthermore, whereas the distinction of the social world into public and private spheres is presented as a natural division, it is rather

> 'a powerful ideological tool, reinforcing as natural and inevitable a set of structural inequalities between groups of people – men and women, adults and children – and favouring the interests of some groups at the expense of others, as well as legitimating the dominance of some individuals over others at a more personal level' (Sapsford 1999; as quoted in Madanipour, 2003, p. 83).

The way these two spheres are divided can serve as a mirror of social relations and particular socio-cultural contexts, representing a more or less desired balance between the individual and society. This is in line with the view that public space is not a naturally given container and external backdrop to human and social action (which could answer the question of what *is* public space), so that the discussion on 'public space' needs to begin with a more general discussion of the 'public sphere' and its relation to the 'private sphere'.

The qualities of public space as 'public', namely, do not only depend on the forms of the space itself or what happens within it, but on the way that the distinction between public and private is made (Brain 1997; as quoted in Blomley, 2005, p. 281). This distinction affects individuals' mental states, regulates their behaviour, and

superimposes a long-lasting structure onto human societies and the spaces they inhabit (Madanipour, 2003, p. 2). Used as a binary model of social structure, the public-private distinction can and does obscure the depth, breadth, and importance of various types of interactions in everyday life as a field of practices that weaves these realms together (Hansen, 1997, p. 269). This sharp split between the two realms (as seen, for instance, in Bobbio's definition) has been described as one of the defining characteristics of modernity, revealing a sharpening polarization of social life between an increasingly impersonal 'public' realm (of the market, modern state, and bureaucratic organisation) and a 'private' realm of increasingly intense intimacy and emotionality (the modern family and romantic love) (Weintraub, 1997, pp. 20–21). However, in practice this divide seems more fluid, as persons seem to live in much more complicated, fluid and hybrid worlds (Blomley, 2005, p. 294), especially in view of the rapid technological development that has permeated all aspects of our lives. In order not to obscure these shades of *publicness* and *privateness*, which render value for privacy in public space, the specifics of the private and the public realm, and particularly the relationship between them, need to be examined in more detail.

Weintraub (1997, p. 2), one of the most esteemed scholars of the public/private distinction, noted that the distinction is not unitary, rather, it is protean: it comprises a complex family of oppositions, neither mutually reducible nor wholly unrelated, that emerge from different theoretical fields and languages of discourse (each with its own assumptions and connotations). First of all, there are two fundamental – and analytically quite distinct – kinds of imagery in terms of which 'private' is commonly contrasted with 'public' at the most general level: the first is 'visibility', pertaining to what is hidden versus what is open, revealed, or accessible; and the second is 'collectivity', relating to what pertains only to an individual, versus what is collective or affects the interests of collectivity of individuals (*ibid*., p. 4). Public can then refer to collective activity that is visible but also collective activity that is hidden. In this sense, the issue of visibility is irrelevant in itself, as the main focus is on a collective benefit. In regard to the criterion of visibility, public space is equated with scrutiny and control, which is in line with Arendt's (1998, p. 72) perspective on the public realm as a realm, where things are and should be shown (as opposite from the private realm, where things are and should be hidden). These two simple but underlying imageries inform our intuitive understandings of what counts as public and as private most, despite the fact that they are often used in shifting and even contradictory ways.

In scholarly debates, however, more sophisticated models of the public-private distinction are found. Weintraub (1997, p. 7) identified four general models of the distinction in political theory (very influential also among geographers; see Iveson,

2007). The first is a liberal-economistic model in which publicity is associated with the state and privacy with the market; the second, is the republican-virtue or classical model that sees the public sphere as community and citizenship as distinct from the state and the market; the third is a model of sociability in which publicity is defined in terms of self-representation, display and performance, and the private realm of increasingly intense intimacy and emotionality (including the modern family and romantic love); and, finally, a feminist model, in which the public refers to the state and economy while the private refers to the domestic and familial. Following the contemporary discussion in privacy theory, which has begun to emphasise the social and even political value and dimension of privacy, I will focus on the second and third model in this Chapter, seeing the public sphere as a realm of politics and sociability. As such, these perspectives can offer most insight for the topic of privacy in public. I will first, briefly examine the private sphere, and then focus on the public sphere and public space.

3.1 Private sphere: the realm and space of the intimate and the personal

In common modern usage, 'private sphere' indicates a part of life that is under control of the individual in a personal capacity, outside public observation and knowledge, and outside official or state control (Madanipour, 2003, pp. 40–41; Parkinson, 2012, p. 50; Staeheli & Mitchell, 2004, p. 151). In the abstract, it refers to a sphere of negative freedoms, a sphere free from governmental or societal interference, in which political ideals can be constructed and autonomous citizens are nurtured (J. L. Cohen, 1997; Elshtain, 1997). In line with this view, much of the private sphere unfolds in private spaces and the home is widely considered the primary symbol and materialisation of the private realm.

However, private life can play out also outside of private territories, such as in a public library or in a park. It follows that private space is an individuated portion of social space, a space that individuals enclose to control for their exclusive use (Madanipour, 2003, p. 68). It provides a physical home-like environment for the body with its mental or portable personal spaces. Aside the inner private space of the mind (which is highly dependent on the physical body to grasp the outer world), lies personal space, the invisible, mobile and subjective space around the body, functioning as the extension of the body. It includes spaces that are personalized by people who inhabit them (such as apartments, hotel rooms, workplaces, cars, computers and mobile phones) and the processes through which this personalization occurs (Parkinson, 2012, p. 54; Sommer, 1969). It is 'a social institution in the sense that the observation of personal space depends on the perceived sense of the self and of the appropriate behaviour in public places' (Madanipour, 2003, p. 31). Thus, personal space can be described as 'a small

protective sphere or bubble that an organism maintains between itself and others' (Hall, 1990, p. 119), which individuals carry with them wherever they go.

Personal space functions as a regulatory process through which access to a person is controlled, helping to achieve a desired level of privacy (Altman, 1975, p. 3). Such control enables individuals to create a personal territory, a protective layer from social pressures, which enables them to develop a sense of identity, find a location in the social world and develop as an autonomous political subject (Elshtain, 1997, p. 180) It is essentially a space where opinions may be expressed and actions taken without the fear of state surveillance or sanction and where ideas can be developed and decisions made in relative safety from social pressures (Staeheli & Mitchell, 2004, p. 148). As it does not privilege particular forms of discourse, it may allow a wider range of voices and positions to be articulated (although this has been critiqued by feminists, who argue that the private sphere is – or at least was in the past – a place where men dominate women).[125] Furthermore,

> '[t]he control of enclosed, private spaces offers the individual an ability to communicate with others through becoming a means of expression of their will, identity and power. It also offers them the ability to be let alone by being protected from the intrusion of others. The establishment of a private sphere offers the individual the ability to regulate the balance of concealment and exposure, the balance of access to oneself and communication with others' (Madanipour, 2003, p. 68).

Personal space therefore provides individuals with a *place* in the world and acts as a barrier that protects and distinguishes individuals from the outside world. Parts of this space are legally protected by the right to privacy in various forms, such as protection of the home, communication, personality and personal data, as seen in many international human rights instruments, national constitutions and other laws around the world (see e.g. Koops et al., 2017).

3.2 Public sphere: the realm and space of politics and sociability

At the other side of the spectrum, we find the *public sphere* and *public space*. Public space has traditionally been seen as a shared space that serves as a place to gather and to meet both friends and strangers. The term 'public' therefore connotes the idea that such settings – and activities therein – are accessible to everyone (Altman & Zube, 1989, p. 1; Madanipour, 2003, p. 111). In general, they are places outside the

125 See DeCew's (2015) recent overview; for more, see: (MacKinnon, 1989; Nash, 2005; Okin, 1989; Olsen, 1983; Pateman, 1990; Richardson, 2011).

boundaries of individual or small group control and used for a variety of functional and symbolic purposes (Madanipour, 2003, pp. 112–113). Accordingly, Altman (1975, p. 118; similarly Goffman, 1959) defined public space as a physical space to which almost anyone has free access and occupancy rights on a temporary basis.

Such space is important primarily for two general reasons: first, because it provides a physical space for interpersonal communication and social encounters that make a community possible, and, second, because it represents the *stage* where – visible to others – individuals, groups, and crowds become political subjects (Carr, Francis, Rivlin, & Stone, 1995; Walzer, 1986, p. 470). Two distinct types of collective or public activities that make space into public space and place are: social activities that make public space into a realm of sociability, and, political activities that make it into a realm of politics. In this sense, two general types of conceptualisations of the public sphere that are particularly relevant for public space, and which are often mixed together, can be distinguished: the social perspective, which sees the public sphere as a realm of sociability, and the political perspective, according to which the public sphere is a realm of politics (generally in line with Weintraub's republican-virtue and sociability models, respectively). As they have somewhat different implications for privacy in public space, I will examine both, beginning with the political theorisation of the public sphere.

3.2.1 A political perspective on the public sphere: the realm of politics

A political perspective on the public sphere is probably the most common basis for its conceptualisation. According to this perspective, the public sphere refers to the realm of political community based on citizenship. The political public sphere thus provides individuals an opportunity to engage in political participation through discussion, forming opinions and building consensus, as well as engaging in collective political action to pursue mutual goals (Arendt, 1998; Benhabib, 1996; Habermas, 2015; Lefèbvre, 1991; Soja, 2010; Young, 2000). One of the key political conceptualisations of the public sphere is Habermas' historical and sociological account of the bourgeois public sphere.[126] He understood it as the sphere in which private individuals come together as a public in order to engage in – essentially face-to-face – public and critical use of

126 Habermas' public sphere is rooted in the development of civil society that originated in late medieval Europe. Until then, the public sphere was limited to the nobility and monarchy, who presented themselves *before* the public. The rise of the modern state changed this, so that the public realm became equated with the realm of the state. As the monarchy evolved into the modern state, the public sphere changed from the realm of the court to the realm of the state. In this process, the 'town' (with its coffee houses and salons) started to dominate the cultural scene, as against the 'court' that constituted the focus of literature and art (Madanipour, 2003, p. 173).

reason (Habermas, 2015, p. 27). Thus, the principle of this sphere can be called 'critical publicity' (Madanipour, 2003, p. 174). However, according to Habermas (2015, p. 140), as the public sphere expanded to incorporate new sections of society, it began to erode by losing its political function of subjecting public affairs to the control of a critical public. Moreover, with the development of capitalism, the previous culture-debating public turned into a culture-consuming public, engaging in individuated reception and consumption of cultural products, rather than in public communication and rational-critical debate. In a visionary manner (in view of the present-day phenomenon of fake news and the *Cambridge Analytica* scandal[127]), Habermas claimed that discussion then assumes the form of a consumer item and advertising comes to serve the functions of political and economic propaganda – the public sphere thus 'serves the manipulation *of* the public as much as legitimation *before* it' (2015, p. 178; emphasis in original).

Whereas Habermas focused on the institutional elements of the public sphere, Arendt (1998) emphasised the material aspect in her historical conceptualisation based on the ancient Greek *agora* – physical public space. She saw the public realm as an integration of the social and physical, a material common world. According to Arendt, the public realm is thus an exposed common *space*, where people gather but do not 'fall over each other'. She understood the term 'public', first, as referring to the appearance in front of others – 'everything that appears in public can be seen and heard by everybody and has the widest possible publicity' (writing, of course, before the digital era; Arendt, 1998, p. 50). For her, the public and private realms thus differ in that in the public realm things are and should be shown, while in the private realm they are and should be hidden (*ibid*., p. 72). Second, she understood the term 'public' as referring to the physical space, the in-between of people, which connects and separates persons at the same time. The public realm in the sense of physical public space thus facilitates co-presence and regulates (through its physical limitations) interpersonal relations.

Based on this account of the public sphere, it becomes clear that public space plays a powerful role in the social and political activities involved in the 'making of the public' that constitutes the public sphere by providing individuals a material space to engage in political participation (Mitchell, 2003; Young, 2011). Furthermore, the making of the public also necessarily involves values of plurality, openness and social learning, and activities such as making claims, achieving visibility and recognition, influencing public opinion, establishing legitimacy, contesting the conception of

127 See, for example, Mihailidis & Viotty (2017); Greenfield, P. (2018, March 26). The Cambridge Analytica files: the story so far. The Guardian. Retrieved from https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

the public, renegotiating social and political rights and (group) identity formation (Ruppert, 2006, pp. 277, 280–281). Hence, public space as space *in abstracto* (rather than a concrete place) features personal rights that are both politically and spatially grounded, including the rights to representation, assembly and freedom of action in urban open spaces (Lefèbvre, 1991; Mitchell, 2003). Only in such a sphere of publicness, can citizens develop their deliberative capacities and identities, make claims for recognition, and transform multiple self-concern into a recognised common interest (Koch & Latham, 2012, p. 515; Sennett, 1992a).

Both of these accounts of the public sphere have, however, been criticised as being elitist and able to develop and function only by keeping the majority of the population out (Benhabib, 2000; Fraser, 1990). Fraser (1990), for example, criticised the singular universal public sphere as conceptualised by Habermas, arguing that it needs to be replaced with a theory of multiple contending and often mutually exclusive public spheres. As an attempt to overcome these issues, Charles Taylor (1997, p. 209) conceptualises a 'multiplicity of public spheres nested within each other'. This 'network of nested public spheres' represents a 'topical common space' (*ibid*., p. 209) in which the members of society meet through a variety of media, including print, digital and face-to-face encounters, in order to discuss matters of common interest and, thus, be able to form a common mind about these (*ibid*., pp. 185-186).[128] The role of the nested or multiple public sphere(s) is thus double: on the one hand, they need to allow for a multiplicity of (sometimes contending) ideas and claims, and, on the other, to enable persons to form common opinions and arrive at common decisions. However, the commonality that is created through co-presence is real but limited – the effect of the public sphere is therefore not necessarily the creation of singular outcomes, but the possibility of developing different responses. In this sense, Berman (2006) talks about an 'open-minded public space'.

Public space, then, is the 'space of co-presence and simultaneity, where different actors can be present in the same place at the same time, where individuals can develop freely within a plurality of possibilities that are negotiated collectively' (Madanipour, 2003, pp. 181–182). In this sense, public spaces are sites of contention and instability, the meaning of which always involves a struggle (Mouffe, 2014;

128 A key question thus is, how is it possible for collective decisions to be made so as to reflect genuine self-rule, rather than through manipulation of the mass media and political process by interest groups and elites. This issue, however, goes beyond the focus of this dissertation.

Springer, 2011).[129] This is connected to the idea of 'radical democracy', which (contrary to Habermas) does not aim at establishing a rational consensus in the public sphere, but wants to defuse the potential human hostilities by providing the possibility for antagonism to be transformed into 'agonism', according to which conflict should not (and cannot) be eradicated from democratic societies. According to Mouffe (2014, p. 125), overemphasising consensus, coupled with an aversion to confrontation, 'engenders apathy and disaffection with political participation'. A well-functioning democracy therefore calls for a confrontation of democratic political positions. As such, democracy always runs the risk of violence – but paradoxically – this potential is mitigated by allowing conflict to play an integrative role (Springer, 2011, p. 531). While a certain level of cohesion is, of course, necessary for societies to function, it must always be accompanied by dissent. According to Mouffe (2014), when a society lacks a dynamic public space that allows for agonistic confrontation among diverse political identities, a more nefarious space (or spaces) may open, where alienation fosters alternative identifications along antagonistic divides like nationalism, religion, and ethnicity.

The value of public space in regard to the making of claims thus lies not only in the possibility to participate (requiring access) but also in the possibility of being seen. As such, public space is a space of continuous contestation as well as a space of exposure, representing an arena, where groups (and sometimes individuals) can achieve public visibility, seek recognition and make demands (Ruppert, 2006; Zukin, 1995). There are many examples of people fighting for inclusion as political actors in public space, including suffrage movements, free-speech fights, union strikes, feminist or black activism, and homeless struggles (Mitchell, 1995). Public spaces of democratic societies therefore have a processual and fluidic character – they are constructions to be maintained and repaired as the collective interests are defined and contested (what Agamben called 'a means without end', in 2000, p. 7; also Springer, 2011, p. 542). From this perspective, then, public space is seen – in line with the common view – as a space of exposure.

However, in order to participate in democratic politics, one needs to be seen in a specific way. In fact, one needs to be hidden but in such a way that her voice is heard.

129 It thus is better to think of public space as having an essentially two-sided character, which has assumed widely varying historical forms (Dixon et al., 2006, p. 190). On the one hand, public space has always been conceived as an area of order where 'appropriate' publics might participate in a particular ideal of urban existence. On the other hand, public space has also been conceived as a site for oppositional activity, playful deviance, and educative exposure to the full range of people and values that make up a society.

The idea is not that persons are or should be individually identifiable (except, indeed, when an individual seeks personal identifiability in order to secure a personal claim). Quite the opposite, a certain layer of obscurity (often referred to as anonymity)[130] particularly in relation to the state, is required in order to perform many of one's political rights, particularly of dissent. This connects to the way that Arendt (2006) used the Greek concept of a mask as a way to facilitate the implementation of the democratic condition of plurality. She saw it as a specific way in which unique human identities and voices penetrate the public space (cf. Agamben, 2011; Kudina & Baş, 2018, p. 126; Nagenborg, 2017). As she put it: 'The mask as such obviously had two functions: it had to hide, or rather to replace, the actor's face and countenance, but in a way that would make it possible for the voice to sound through' (Arendt, 2006, p. 106).[131] In more recent debates, scholars have begun to use the concept of anonymity in order to debate political participation in public space.

Like the mask, anonymity can be said to have both identity-negating as well as identity-forming features. Concealment of one's identity is seen as particularly important in political participation in public space. The identity-negating aspect of anonymity thus protects the individual from interference of powerful actors (either public or private) and peer pressure. However, anonymity is also inherently communicative and thus identity-forming (Asenbaum, 2018, p. 1; cf. Nagenborg, 2017). As such, anonymity is not only or primarily about hiding; quite the opposite, it is a matter of showing, exchanging opinions, and creating specific identities that we show to others. Echoing Arendt's thoughts on the mask (where the voice sounds through the mask hiding the face), Assenbaum (2018, p. 11) talks about 'absence as presence in the public sphere'. Anonymity shields the identity (at least the idem type of identity, e.g. as found in our passport; discussed in Section 3.1.1 of Chapter 3) *while communicating content* in the public sphere. Therefore, anonymity enables the self-expression of a democratic subject.

3.2.2 A social perspective on the public sphere: the realm of sociability

The public sphere has also been theorised as a sphere of sociability (see for instance Ariès, Duby, & Chartier, 1989; Elias, 1978; Jacobs, 2011; Whyte, 1988). While this aspect of the public sphere is often considered to play a minor (or side) role compared to the political approach, I will consider it separately and in detail, in order to elucidate its distinct implications, especially for privacy in public space.

130 I explain the difference between the two terms – obscurity and anonymity – in Section 3.3.

131 Or as Nagenborg (2017, p. 50) put it: '[T]he mask is a *claim* for another (non-)identity. It signals the desire *not* to be recognized as a specific individual.'

The social perspective on the public realm sees the public realm not as the *impersonal* realm of the state or the market exchange (a realm of bureaucracy and the legal contract) but as the *interpersonal* realm of community and sociability – the realm of meaningful, as well as instrumental, face-to-face social encounters. In this sense, some have argued that it is a realm that stands in between the public and the private realm, so that it is can be interpreted as private (when in opposition to the impersonal) and at times as public (when in opposition to the personal or private) (cf. Lofland, 1998 distinguishing between private, public and parochial realms; Madanipour, 2003, p. 110).[132] From this, one can already imagine the public and private spheres not as a dichotomous distinction of unitary and exclusionary realms but rather as a number of dimensions and layers of privateness (or privacy) and publicness (Madanipour, 2003, p. 108; more on this in Section 3.3). This also implies a shift from *space*, as a site of potentiality and abstraction, to *place*, a location defined by the meanings attributed to it by its users. In this sense, public places have also been described as 'third places' (Oldenburg, 1999) – social gathering spots that lie between the home and work, providing individuals with the opportunity to form bonds with each other and with the location itself (Duneier, 1994; Milligan, 1998). Public places therefore serve as the basis for individual and place identity, and form the foundation of local culture and community (Zukin, 1995; discussed in more detail in Section 5).

It is clear from this that in regard to sociability, public space plays an essential role, as physical public space is needed in order for face-to-face encounters between strangers and acquaintances (all of those who are not a part of one's intimate circle of the household or friends) to occur. Public space thus serves key social functions, enabling interaction and practices of sociability. Social interactions in public places are an integral feature of an associational society (and individuals), the informal web of civic relations that characterises our 'life between buildings' (Dixon, Levine, & McAuley, 2006, p. 187; Gehl, 2011). Scruton (1987, p. 13) described it as 'a sphere of broad and largely unplanned encounter[s]', as fluid sociability among strangers and near-strangers. The public sphere is hence an environment that encourages mingling and encounters between people of different classes, races, ages, religions, ideologies and cultures and, as such, serves as a breeding ground for mutual respect, political

132 Arendt (1998), for example, conceived of the 'social realm' as a realm alternative to both 'the private' and 'the public'.

solidarity, tolerance and civil discourse (Walzer, 1986).[133] Public space within this vision of the public sphere is thus a space of heterogeneous existence and a space of symbolic display, rather than of conscious collective action (which forms the political public sphere); it is a space of 'physical proximity coexisting with social distance' (Weintraub, 1997, p. 25).

The ideal of public space as a space of sociability is thus embedded with values of plurality, openness and social learning. Its function is to make diversity agreeable or at least manageable (Scruton, 1987, p. 23). Such sociability enables a 'wealth of public life' (or 'social capital' as Jacobs called it), a multi-stranded liveliness and spontaneity arising from the ongoing intercourse of diverse individuals and groups that can maintain a civilized coexistence (Madanipour, 2003, p. 165). Of course, this is also possible because behaviour here is regulated by a range of social codes and conventions, forming the characteristic virtue of this form of public space – civility. With the help of social codes and conventions, public space becomes an environment, which facilitates the development of trust and the possibility of action outside the state remit and control. This is essential, as only through a certain level of trust social public life is possible (Dixon et al., 2006, p. 188).

This relates to the question, how individuals make sense of each other and how they can relate to one another, which is at the heart of social life. The meeting of different subjectivities in common space results in a social world in which meaning is constructed through intersubjective relationships. As Madanipour (2003, pp. 165–166) put it:

> 'Public space allows us to experience other people's presence and get to know their viewpoint, which is an essential ingredient of living in human societies. It is impossible for me to see the world entirely from the viewpoint of another person and I am not able to enter the private realm of strangers and experience life from their perspective. I can, however, albeit in a narrow sense, have the same perspective as they might have in public space. I can stand where they stood and experience common space from the same perspective, even though my experience may be completely different. If we are all present in the same space, I will be able to share the same street corner with the

133 While digital social media, of course, also enable the meeting of strangers, this possibility might be more constrained due to the way these media function. For instance, due to the 'filter bubble' effect, we are much more likely to be shown messages or persons whose views are generally in line with our own views. This can also be (ab)used for purposes of affecting democratic political processes, as can be learned from the Cambridge Analytica example (see ref. 121).

> residents of private realms, looking at the city from the same angle. The space we share, therefore, allows us to share an experience of the world around us. This is, however, temporary and limited. Nevertheless, it is more than a mere visual experience of looking onto the same physical reality from the same vantage point; it is, rather, part of a multi-layered experience of the presence of others.'

By being present in the same place with others, shared experience of the world becomes possible and a link is made with previous generations who experienced (or future generations who might experience) the same physical reality. This connecting role that bridges time endows public space with a certain permanence.

The codes and conventions that informally regulate behaviour in public places can, however, also function in a repressive manner, stifling social difference, rather than enabling it. Already Mill (2016) warned against the effects of social pressure, promoting a form of tolerance (see Chapter 3). That is why Hansen (1997, p. 193) emphasises the informal rules and fluid negotiation in the sphere of sociability and community. Public space here again plays an essential role. Precisely the openness of accessibility and flexibility of use of public spaces – the park, the street and the square, but also the neighbourhood, bar and café – allows for a fluidity of negotiation. No single person or small group can (at least ideally) limit these personal rights (to the city, as Lefèbvre put it). A significant degree of flexibility is hence needed in order for the public space of a city to become and remain an interpersonal space of sociability. Space is needed for a variety of performances by different actors in different conditions and for different reasons. Whereas a public space may have been designed and organized for a particular social ritual, such as an annual festival or religious and state parades, it can become the setting for a whole range of other, less specified activities throughout its life. Similarly, a place may have been created as the setting for a particular routine during the day, such as a marketplace, but left to be used in another (less restricted) way at night, when it can be taken over by different routines and activities. Echoing Mouffe, Sennett (Sennett, 1992b, p. 132) argued that a level of disorder and difference in the city is needed, because it forces us to engage with 'otherness', to go beyond one's own defined boundaries of self. Without a certain level of disorder and difference people, namely, do not learn to deal with conflict so that if and when conflicts do arise, they tend to be more violent (giving the example of road rage).

These 'open' and flexible (in the sense of being multi-functional and somewhat disorderly) public spaces should thus be differentiated from other places in the city, which have a particular functional significance and are usually closed off to other types of use (e.g. restaurants, museums, libraries and theatres). The interpersonal character

of public space is thus influenced by the ways in which the configurations of physical space facilitate, channel, and block the flow of everyday movement and activity (Whyte, 1988). Of course, successful public space also relies on a range of political and economic resources: from the more mundane, such as trash collection, street cleaning and policing, to the making of laws and policies that regulate surveillance in public space. The public space of sociability thus emerges from a complex interplay of spatial and social arrangements (Weintraub, 1997, p. 23). This includes a limited level of visibility or exposure that preserves a layer of trust that is required for social public life in the city to occur, rather than complete transparency that is often assumed about public space. This is especially so, if we want to preserve the multi-functionality of public space and a healthy layer of disorder, difference and unpredictability. The idea that everything should be out in the open is childish, as Nagel (2002, p. 9) put it. Instead, a balance between concealment and exposure is the key to a sociable public space. The technological transformation of public space (as is taking place particularly with the transformation into smart cities and living labs; see Chapter 1), where everyone is under various types of surveillance most of the time, however, could lead to a noticeable decrease in sociability and a withdrawal into private spaces and silence as the best or only form of protection.

3.3 A layered approach to the public-private distinction: shades of privateness and publicness

Geographers and scholars from other fields, particularly feminists, have been arguing for decades that the private and the public are inherently complex cultural categories, the boundaries of which are shifting, porous and unstable (Kumar & Makarova, 2008, p. 324; Weintraub, 1997; see also the discussion on the etymology of the term private in Chapter 3). This is clear when we observe the wide variety of ways in which what we have come to think of as 'private' and 'public' spaces, behaviour and practices were both linked and separated at different times and in different places in the history of Western society (see Ariès & Duby, 1988; Ariès et al., 1989; Ariès, Duby, & Perrot, 1990; Ariès, Duby, & Prost, 1991). In fact, the line separating the public from the private has never been rigid. Rather than being separate, the two spheres are in constant interaction and reciprocity: they are both interdependent and intertwined. As such, they are mutually constructed: publicness and privateness (or privacy), along with public and private spaces, are defined in relation to each other, so that the relationship is 'multivalent and may shift over time and across different settings for different social groups' (Koops & Galič, 2017, p. 32; similarly Kumar & Makarova, 2008; Madanipour, 2003; Staeheli & Mitchell, 2004). While the public sphere has been theorised as the space of politics, it is also a space that is also constituted in and through privacy

(Staeheli & Mitchell, 2004, p. 151). As Elshtein (1997, p. 180; emphasis in original) put it:

> '[T]he public world itself must nurture and sustain a set of ethical imperatives that include a commitment to preserve, protect, and defend human beings in their capacities as private persons, *as well as* to encourage and enable men and women alike to partake in the practical activity of politics. Such an ideal seeks to keep alive rather than to eliminate tensions between diverse spheres and competing values and purposes. […] Only in the space opened up by the ongoing choreography of [public and private] can politics exist – or at least any politics that deserves to be called democratic.'

Since public and private are interdependent, shifting the boundaries in the private sphere causes a rearrangement of public spaces of sociability and democracy, and *vice versa*. In this sense, Jacobson (2010) argues that human beings are not first or most originally 'public' beings, rather we must develop the behaviours and attitudes necessary for citizenship. This is something we can only do by emerging out of our familiar, personal territories – our homes, into the open – into public space. Thus, if there is no public space (as a part of the public sphere) into which one can (more or less) freely venture and participate in the various activities of politics and sociability, a person cannot fully develop into a citizen or a community member (and, consequently, his personal development is limited as well).

Furthermore, rather than seeing the separation of the public and private spheres as a binary opposition, one should see it as an intertwined or interwoven relationship of spaces, where the two realms meet through shades of privacy and publicity (Madanipour, 2003, p. 239). The private and the public, then, exist on a continuum. Furthermore, in line with contemporary perspectives on the plurality of public spheres, this continuum is formed of different layers of public and private spheres and spaces, which are not fixed. Some of these evolve into others without necessarily the first one disappearing, some are entirely located within the other (e.g. a public sphere of private people within the private sphere), while others are tangentially

connected (e.g. the state public sphere and the private 'authentic' public sphere).[134] The picture that emerges, is therefore one of multi-layered, overlapping spheres that have at times a tense relationship with each other and in any case are always changing and evolving (Madanipour, 2003, pp. 175–176). Public space is thus made of layers and dimensions of privateness and publicness. In between the two realms thus lies a series of gradations – 'liminal' spaces – where the private and the public collide (Blomley, 2005, p. 294; Parkinson, 2012, p. 53). Public space as 'layered space' includes many layers of private, semi-private, semi-public and public spheres – referring to spaces, persons and activities (and the same goes for private space). This means that public spaces can be used for essentially private activities, such as kissing and having dinner with one's partner, for essentially public activities, for instance, demonstrating and striking, as well as for various activities in between, including planting trees in a community garden.

Such a relational approach to the public and private sphere also leads us to think of public space not only as a space of exposure but also as a space of obscurity. I prefer to use the term 'obscurity' here, rather than the more commonly used term 'anonymity', as obscurity refers to a more limited type of *hiddenness* – a state of being relatively unknown and not prominent, somehow shrouded and, thus, not clearly seen or easily distinguished. In contrast, anonymity refers to a state of complete unrecognizability and unidentifiability.[135] This need for obscurity public is also confirmed by both the political and the social perspective on the public sphere.

Despite this layered (rather than oppositional) approach to the public-private distinction, modern technology seems to have substantially changed the way the

134 Some scholars (e.g. Gal, 2002) have gone even further, arguing that the relationship between the public and the private is a communicative phenomenon taking the form of a fractal relationship. As such, 'public' and 'private' are not particular places, domains, spheres of activity, or even types of interaction; even less are they distinctive institutions or practices. As Gal (2002, p. 81) put it, the public/private dichotomy is a fractal distinction – a particular kind of indexical relation. 'Thus, whatever the local, historically specific content of the dichotomy, the distinction between public and private can be reproduced repeatedly by projecting it onto narrower contexts or broader ones. It can also be projected onto different social "objects" – activities, identities, institutions, spaces and interactions—that can be further categorized into private and public parts. Then, through recursivity (and recalibration), each of these parts can be recategorized again, by the same public/private distinction' (*ibid*.).

135 See for example the Merriam-Webster dictionary on 'obscure' and 'anonymous': Obscurity. (n.d.). Retrieved March 21, 2019, from https://www.merriam-webster.com/dictionary/obscure#h1; Anonymous. (n.d.). Retrieved March 21, 2019, from https://www.merriam-webster.com/dictionary/anonymous.

private and public are practiced and protected. In the not too distant past, privacy could be secured through the physical barriers of walls, doors and curtains, and the spatial limitations were dictated by being in a particular place at a particular time. Hence the walls and gates could regulate the publicity and privacy fairly effectively (Madanipour, 2003, p. 47). Some of what happened behind the walls could be known to the outsiders, but only those who lived locally, in the same street or village. It could spread farther, albeit very slowly and in distorted forms, only if the person involved was very significant. Now, on the one hand, it is increasingly possible to see *inside* the private space from the outside (public space; at least, by examining what is emitted from the inside) using various technological means, including sewage analysis, heat imaging, video surveillance via drones, hacking and so on.[136] Furthermore, the information gathered in this way can be communicated to the rest of the world via ICTs in an instant.

On the other hand, there is also an increase in possible new technological ways of being read or sensed in public space, over distance and time, so that our 'being in public space' is changing too. This has been termed the 'domestication of public space' (Kumar & Makarova, 2008, p. 325), as many things once done at home, such as eating, talking intimately, expressing emotions, entertaining oneself, are now increasingly done outside the home. While nothing is ever *truly* public or *truly* private, we always strive to present ourselves based on what we feel to be 'situationally appropriate' (Ford, 2011, p. 560). This is, however, increasingly difficult to achieve nowadays, when we unwittingly give off an expanding array of *expressions* in the sense of (meta)data that are generated via digital technologies and by simply being physically present in public space. This is so because we carry smart phones, laptops and wearable computing device – each of which potentially contains large amounts of private data – with us, when we exit our homes. Furthermore, sensing technology is increasingly embedded into the public space itself, for example, smart CCTV, wifi tracking technology and sound sensors. These technologies are in constant *communication* with the technology we carry with and on us. For example, our smart phones often connect to wireless networks that are provided by private companies or the municipality automatically, thus bringing all sorts of private data – that would otherwise be safely stored in private places, inaccessible to others – into (virtual) public space (Timan et al., 2017a, p. 1).

136 E.g. Karantzoulidis, S. (2018). How Advancements in Thermal Camera Tech Are Heating Up Opportunities. Retrieved March 31, 2019, from https://www.securitysales.com/surveillance/advancements-thermal-camera-tech-opportunities/; microMole - sewage monitoring system for tracking synthetic drug laboratories. (2015). Retrieved from https://cordis.europa.eu/project/rcn/194878/factsheet/en.

In this sense, some have claimed the emergence of 'new geographies of privacy and visibility' (Ferreira, 2015, p. 161). The electronic media have been widely characterized by their ability to reorganize the boundaries between public and private spaces that affect our lives, not so much through the content but changing the 'situational geography' of social life (Meyerowitz, 1987, p. 6). Many have thus claimed that the spatial reorganisation of society and culture around ICTs has led to a fundamental shift or blurring of boundaries between public and private, so much so that there is an increasing difficulty of recognising any boundary at all (Ilouz, 2007; Kumar & Makarova, 2008). However, the private and the public have always existed among shades of privateness and publicness, so that both public and private space are essentially layered spaces. Consequently, public space should be thought of both a space of exposure and a space of obscurity. While these layers of exposure and obscurity have been existing for a long time, new, additional layers of both are now emerging through the developments in technology. However, because of the common (mis)understanding of *public* as only visible or exposed, the emphasis is on the new possibilities of making the private visible and the public hyper-visible (Donath, 2014). This can be seen in recent practices in law enforcement and, increasingly, in the actions taken by other public and private actors (such as tax authorities, technology companies, shops and restaurants) tracking our actions in public space for various purposes.[137] If we are to preserve public space as both a space of exposure and obscurity (which plays an essential part in the complex public-private relationship), the increasing technological possibility to make people and their behaviour – both in public and in private – more transparent should be regulated in a more sufficient way than has been until today (I further address this need in Chapter 7).

4. CONTEMPORARY POWER SHIFTS IN PUBLIC SPACE: PRIVATISATION AND SECURITISATION OF PUBLIC SPACE

In line with post-structuralist and radical geographers, who see space as inherently caught up in social relations, where physical spaces and the social life of citizens are shaped together, contemporary shifts in power regarding public space can be analysed. In this sense, spaces are seen as being *made* through emergent patterns of use, their individual and social functions, and power relations (Koch & Latham, 2012, p. 517). It is thus essential to ask questions relating to power such as: how

137 See, e.g. Naafs, S. (2018, March 1). "Living laboratories": the Dutch cities amassing data on oblivious residents. The Guardian.

are public and private spaces shaped; who has access to them; what sorts of norms govern them; and how are the actions that develop in it spread across geographical networks of communication? Power, as I understand it here, roughly comes down to someone being able to get another to do something that the other would not otherwise do. This, of course, does not only involve brute force, but also limiting the other's decision-making space (e.g. through agenda-setting) as well as using cultural, institutional and architectural mechanisms that have a disciplining effect (Bachrach & Baratz, 1962; Dahl, 1957; Lukes, 2005). The construction of public space and place, which I will examine bellow, demonstrates well how such mechanisms are used in power relations.

Particularly since the 1990s, the ongoing transformation of urban public space, including shifts in design, management, financing, and the proliferation of (increasingly digital) surveillance, has emerged as a key focus of geographical concern. Building primarily on the political and social notions of public space and their value for the practice of democracy and sociability, many geographers have (usually critically) observed two trends: the *privatisation* and *securitisation* of public space.

4.1 Privatisation of public space

Privatisation of public space refers to the commercialization and commodification of the public sphere (understood in a socio-political way) resulting from the domination of private, neo-liberal interests over the provision, regulation and maintenance of public space (Kohn, 2004; Mitchell, 2003; Soja, 1996; Sorkin, 1992b). Since the end of the 1980s, for a number of socio-political and budgetary reasons, many states (especially in North America and Western Europe) have ceded many of its core functions concerning the regulation of public space to local governments (particularly municipalities) and, increasingly, the private sector (Brotchie, Batty, Blakely, Hall, & Newton, 1995; Fyfe & Bannister, 1998; Loukaitou-Sideris, 1993; Van Melik, Van Aalst, & Van Weesep, 2009b). According to Fyfe & Bannister (1998, p. 257), de-industrialisation and rapid growth of out-of-town shopping centres and business districts lead to the dereliction of many central urban areas and growing fears about the economic and social consequences of this spatial reorganisation of economic activity. Because of the shift of the economic base, from manufacturing industry to the service sector and high technology industries (which are far less attached to localities than the heavy industries of the past), the role of cities needed to be redefined. Rather than concentrations of blue-collar workers in industrial cities, service cities are concentrations of white-collar workers with their very different needs and expectations. As localities and regions began to compete in the world economy to attract the increasingly mobile capital, they needed to create safe and attractive environments for the investors and their employees (Hall, 1995).

Furthermore, local authorities also began to improve the quality of city environments to attract tourists.

This transformation involves private construction, funding, management and security of public spaces, which, many have argued, has transformed these into *privately owned public spaces* (POPs), also called semi- or quasi-public spaces that look public but are not (in the sense that the rights connected to public space are severely curtailed) (Harvey, 2008; Mitchell, 2003). Contemporary cities are rich in new types of public-seeming spaces, such as shopping malls, corporate open spaces (plazas, parks, gardens), business and innovation districts (BIDs), and gated communities.[138] In contemporary public and quasi-public spaces, an extending array of activities are forbidden: taking pictures without a permit, giving speeches, rough sleeping, drinking a beer on the grass or having a picnic with wine in the park, as well as dissenting in a variety of peaceful ways (Van Eijk, 2010; Weaver, 2014).[139] Kohn (2004, p. 3) argues that due to the growing phenomenon of private government, public space is disappearing and public life (including democratic practices) is undermined. The main issue here concerns the extent to which rights and liberties connected to public space, including rights to representation, assembly and freedom of action in urban open spaces, can be safeguarded when ownership and management is distanced from democratic forms of control (Koch & Latham, 2012, p. 521).

As space is stripped of its emotional and cultural value that is developed through people's use through time, it is treated as a mere commodity. Investors are, namely, interested in a safe return on their investment. The creation of new types of public space is thus driven by the desire to ensure that spaces are safe, lucrative, predictable and, all in all, tightly defined. Corporate producers of space seem to see the public as a homogeneous mass and a passive market receptive to commercial consumption of the city (Silver, 2014, p. 3). Consequently, social action in such spaces is tightly scripted and prescribed, and behaviour becomes standardised (Madden, 2010). This results in significant restrictions of behaviour, with rules that secure the boundaries of acceptable behaviour within a space now increasingly governed by private entities controlling these quasi-public spaces (Weaver, 2014, p. 3). Just think of the broad manner in which 'escalated behaviour' was defined in the *De-escalate* project by private

138 For more on BIDs, see M Steel & M Symes (2005); Weaver (2014).

139 Also see Garrett, B. L. (2015, August 4). The privatisation of cities' public spaces is escalating. It is time to take a stand. The Guardian. Retrieved from https://www.theguardian.com/cities/2015/aug/04/pops-privately-owned-public-space-cities-direct-action.

actors and scholars from TU/e (that is, not elected representatives of the public; see Chapter 1).

This also implies a loss of contextualization and leads to what Sorkin (1992a, p. xi) calls 'a city without a place attached to it', a city comprised of 'themed spaces'. Such spaces are de-particularised, no longer acting as sites of community and human connection, and increasingly look alike (shopping malls or city squares in Rotterdam and New York are strikingly similar); they become 'non-places' (Augé, 2009). These developments clearly imply a limitation on the role of public spaces as sites of politics and sociability. Furthermore, local governments and private actors practice a form of management and control of flows of populations, making public space (feel) safer in order to maximize the number of visitors, to attract more advertising, to stimulate consumption and to facilitate spending (Harcourt, 2014). This results in repressing all forms of *deviancy* (understood differently at different times and in different places). Such a city, with its new types of privatised public space, is thus closely connected to the second trend geographers have observed – the *securitisation* of public space.

4.2 Securitisation of public space

The *securitisation* of public space refers to the decline of openness, accessibility and flexibility of public space due to the exercise of political power by both state and private actors who are increasing their control and policing of public space (Neal, 2010). A growing range of conducts, activities, political practices and wide-ranging groups of 'undesirables' are being excluded not only from privately-owned but also from state-owned public spaces (Johnstone, 2017; Moeckli, 2016; Ruppert, 2006). Hence, public space – including social and political activities that make up public life – is constituted not only through ownership but also through a wide range of regulatory practices, such as laws, regulations, urban design, surveillance and policing.

Despite the common political discourse on public space that emphasizes its accessibility and openness (the ideal of public space), concrete public space is neither free and democratic nor repressed and controlled – it is both at the same time: '[i]t is simultaneously a space of political struggle and expression and of repression and control' (Lees, 1998, p. 238). Public space thus has an essentially two-sided character, which has assumed widely varying historical forms (Dixon et al., 2006, p. 190).

While exclusion and repression are clearly not new phenomena, we are arguably witnessing new forms of exclusion and control in public space. These are based on a changing conception of the public and a reconfiguration of liberty that exclude certain non-criminal conducts, activities, groups and political practices and that are

increasingly based on preconceptions, prejudices, and fear of potential harm rather than real danger (von Hirsch & Shearing, 1999). In the securitised city premised on a need for surveillance and control over behaviour, public space is secured *from* the public rather than *for* it (Vale 2005, as referenced in Marcuse, 2006, p. 922). As Young (2007, p. 59; emphasis in original) put it:

> '[t]he late modern world celebrates diversity and *difference*, which it readily absorbs and sanitizes; what it cannot abide is difficult people and *dangerous* classes, which it seeks to build elaborate defences against.'

This has led some to declare, rather dramatically, the 'militarisation' (Davis, 2006; in the case of Los Angeles) and the 'end of public space' (Mitchell, 2003).

However, such claims have also been criticized for having an idealized and nostalgic view of the golden days of public space, and for presenting too bleak a view of public space as a site of contention where people are excluded and dominated and as an institution that is disappearing as quickly as democracy itself. Some theorists and geographers, such as Jacobs (2011) and Whyte (1988), hold a relatively optimistic approach to public space, which recognises the evolution of public spaces, where old forms may disappear, but new forms are being created, and treats conflict in public space as a challenge to be overcome by improved design. While this certainly holds to a certain degree, several new mechanisms of control in public space have been developed recently, which might shift the balance between control and freedom more noticeably. The simplest form is found in 'sadistic street furniture', such as barrel-shaped benches, sprinklers, spikes and decorative enclosures, designed to keep homeless and youth away from specific areas (Davis, 2006, p. 226). More recently, with the devolution of power from the state to local governments, attempts of creating 'security zones' or 'security bubbles' (Mitchell, 2003, pp. 43–51; Németh & Hollander, 2010) can be seen, a part of innovative mechanisms of 'preventive justice' underpinned by criminal sanctions (Ashworth & Zedner, 2014; Johnstone, 2017) (and sometimes accompanied by a resurgence of punitive models of 'law and order' governance; Brown, 2004, p. 204). These include widespread surveillance and new public nuisance laws, including legal instruments such as dispersal orders and public space protection orders (PSPOs).

These relatively recent legal tools aim to exclude an increasingly wide range of activities including, smoking, drinking alcohol,[140] rough sleeping (i.e. sleeping in public space),[141] walking dogs and many sorts of behaviour that can be labelled 'rowdy', 'unruly', 'anti-social' or 'escalated'.[142] While such prohibitions are particularly widespread in the U.S. and the UK, they are also being introduced in Europe (e.g. Germany, Switzerland; see Moeckli, 2016, p. 364). A good example of this can be found in the English Anti-social Behaviour, Crime and Policing Act 2014,[143] which allows the use of injunctions (a revised form of the ASBO, transforming it into a wholly civil remedy; Johnstone, 2017, p. 6), dispersal orders and public space protection orders (PSPOs). PSPOs, for example, allow for broad powers of local councils to sanction behaviour (with a fine but where non-compliance results in a criminal offence) that is not normally considered criminal. They are also not directed at individuals; rather, they are geographically defined, making predefined activities within a mapped area prosecutable. Such regulation of public space discourages a wide range of spirited expression (labelled as 'anti-social' or 'escalating') and encourages stereotyped behaviour, clothing and 'social neutrality' in general. Consequently, these practices have the potential to reduce the cities' 'porous, open, intrinsically unpredictable city spaces and systems' to nothing more than an endless series of secured passage points (Graham, 2007). In this way, the required level of disorder and difference that make up the social public life (Sennett, 1992b) is also endangered.

Such practices are a form of security that target what or who is deemed to cause fear, those labelled as 'abject' (Tyler, 2013) or 'difficult' (Young, 2007) – panhandlers, squeegee cleaners, prostitutes, addicts, rowdy teenagers, loiterers, the mentally

140 Drinking alcohol is not allowed in many parts of Rotterdam, for instance, on most streets and parks (regulated in the General municipal ordinance of Rotterdam (*Algemene Plaatselijke Verordering* Rotterdam); Vocke, W. (2018, July). Mag dat: een biertje of wijntje drinken op straat in Rotterdam? Indebuurt Rotterdam. Retrieved from https://indebuurt.nl/rotterdam/gemeente/mag-dat-alcohol-op-straat-in-rotterdam~56763/.

141 E.g. Cromarty, H., & Strickland, P. (2018). Rough Sleepers and Anti-Social Behaviour (England). Retrieved from https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7836#fullreport; Rahim, Z. (2018, October 15). Hungary brings in ban on rough sleeping. The Independent. Retrieved from https://www.independent.co.uk/news/world/europe/hungary-homeless-ban-viktor-orban-rough-sleeping-street-a8584401.html.

142 E.g. Wilding, M. (2017, October). The Age of the ASBO: How Britain Became a Police State. Vice. Retrieved from https://www.vice.com/en_uk/article/gy594q/the-age-of-the-asbo-how-britain-became-a-police-state.

143 Avabilable at: http://www.legislation.gov.uk/ukpga/2014/12/contents/enacted (accessed 31 March 2019).

disturbed and strangers, along with boom-box cars, public drunkenness, reckless bicyclists and graffiti (Johnstone, 2017; Yarwood & Paasche, 2015). Prohibitions of conduct, however, are often based on the proposition that order is only possible by excluding certain people and conduct (Mitchell, 2003). Although the basis for this exclusion is presented as natural or obvious, it is founded on interpretations of what constitutes violence or disorder. Today an incredibly wide array of people and activities typical for them are seen as not belonging in (certain parts of) public space. Although such orders (or laws) are phrased impartially, preventing anyone from, for example, sleeping or lying or sitting in particular public places, they affect almost exclusively those who have nowhere else to sleep or be – that is, homeless people (Moeckli, 2016, p. 364). For example, large areas of Seattle, U.S., have been zoned as 'Stay Out of Areas of Prostitution' (SOAPs) and 'Stay Out of Drugs Areas' (SODAs; covering the whole downtown area). Those convicted of, or sometimes just arrested for, a wide set of offences are required to avoid these zones, and failure to abide by these limits on geographical presence is a criminal offence (Beckett & Herbert, 2008, 2010a, 2010b).[144]

The promise of safety, security and order can hence quickly lead to discrimination, exclusion, displacement or domination (Ruppert, 2006, p. 191), often of specific groups of people, such as certain ethnic groups, immigrants, the poor, the homeless, youths, LGBTQ+ persons, and protesters. Security practices in the controlled city do not seek to modify behaviour but, rather, use space in a territorial way to exclude people or behaviour that is threatening to its imagined values. Often, the discourse around these practices 'links the mere presence of undesirables to "crime", making their eviction a task for the police' (Belina, 2007, p. 324; referring to the ban in Bremen, Germany). As Foucault has observed, space is fundamental to the use of power (Crampton & Elden, 2016; Elden, 2001). The purpose of securing a particular space is to produce a place that is different from those around it. Consequently, as Zedner (2009, p. 61) observes, a complex geography of security is emerging from these practices that encompasses different '"patchworks", "quilts", "bubbles", "corridors", "mosaics", "webs", "networks", and "nodes"' of secure places that extend across different urban spaces in different ways (similarly Hentschel, 2015).

144 Area bans are found also in Europe, for example in the police law of Germany's regions (*die Aufenthaltsverbote*), giving the authorities considerable powers to ban, from a designated zone, anyone reasonably assumed likely to commit a crime (Belina, 2007). In regard to Australia, Palmer and Warren (2014) draw attention to the use of administrative or 'police' laws to exclude problem populations without the need to go through lengthy prosecution processes associated with traditional criminal sanctions.

In a contemporary *secured* or *controlled city*, space usage is therefore increasingly by permit and not by right, and rights can best be exercised at home, in private, effectively discouraging political engagement (Sennett, 1992b) or social encounters with strangers. This desire to purify space of any behaviour that is likely to provoke anxiety and to insulate ourselves from the 'complexities of the city' may, according to Robbins (1995, p. 60), deny 'the emotional stimulus and provocation necessary for us if we are to avoid, both individually and socially, stagnation and stasis'. Such a secured city may thus transform into a 'stagnant fortress' (Smith 1979; as cited in Fyfe & Bannister, 1998, p. 265), standing in opposition to a desired kind of maturity that would make a city able to handle the conflicts that arise there.

4.3 Public space and the law

In view of these transformations of public space, it is important to look at how the law regulates public space and what kinds of limitations it sets for these transformations. As this broad topic exceeds the possibilities in this dissertation, I will only briefly examine it for the purposes of this Chapter.

Given the above diverging and often conflicting meanings of the terms 'public' and 'space', it should not come as a surprise that 'public space' (or its versions in other languages) is not 'a legal term of art, that is, a term with a precise and fixed legal meaning' (Moeckli, 2016, p. 27). Most commonly, legal understandings of 'public space' (or 'public place', as laws seem to use these two terms interchangeably) concentrate on concepts of general accessibility (the opposite of 'private space' or 'private property') and use, rather than considering ownership as the basis of what makes a place public. This understanding is found in numerous definitions of the term as contained in relevant laws regulating the use of public space.[145] Section 35(10) of the English Anti-social behaviour, crime and policing act 2014, for example, defines a public place (in relation to the dispersal of persons from such places) only in relation to access. A public place is 'any highway … and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission'.[146] Similarly, but adding the characteristic of general use, the Irish Criminal Justice (Public Order) Act (Part II, Art. 3) defines public places as outdoor areas but also premises or other places

145 While a definition of a 'public place' can be found in many types of law, the definitions that are most relevant for this Chapter are those found in criminal statutes and other laws that regulate the keeping of public order.

146 The same definition is found in s. 16 of the English Public Order Act 1986 (available at: http://www.legislation.gov.uk/ukpga/1986/64/contents), in the context of processions and assemblies.

to which members of the public have or *are permitted to have access and which is used for public recreational purposes* (including highways, cemeteries and churchyards; my emphasis).[147] In the Netherlands, the focus is on use, so that a public place ('openbare plaats') is a place that is designated as such in the law or if it is *used as such in common practice* (Art. 1(1), Wet openbare manifestaties 1988; my emphasis).[148]

As these examples show, access to (and consequently use of) public space may be restricted, for instance by payment or with other restrictions (e.g. prohibiting persons younger than 16 or 18 to gather there in between certain hours).[149] Therefore, diverse types of state, collective or private property with regulated access, including obligatory payment for access, are considered legally as public places. However, as (post-)structuralist geographers have shown, the division of the social world into public and private is not a natural division; rather it is an expression of power. Since quasi-public space is subject to a private-law regime, members of the public do not have a legal claim to be granted access to it or to use it in a manner contrary to the wishes of the owner. The extent of limits on the owner's discretion is as yet uncertain, as the case law on this question is as yet unclear.[150] Generally, courts still seem to treat diverse semi-public spaces in the same manner as any other private property (Moeckli, 2016, p. 57).

Moreover, since the public and the private spheres are interdependent and constitute each other, the implications of privatisation and securitisation of public space for privacy also require reflection. Public spaces should not be conflated with public actions, nor should private spaces be conflated with private actions. Certain private actions are, and always have been, performed in public, protected by the layer of

147 While laws in Switzerland do not use the term 'public space/place' at all, government guidelines for the improvement of safety in public and semi-public space of the City of Zurich define 'public spaces' as 'streets, paths, squares, public buildings and other spaces, which are open for the free use of the public' (as quoted in Moeckli, 2016, pp. 29–30). This definition then also applies both the characteristic of common access and common use (although with somewhat different wording).

148 Available at https://wetten.overheid.nl/BWBR0004318/2010-10-10 (accessed 31 March 2019).

149 Such youth exclusion measures are found in several countries, including the UK, U.S. and Switzerland (Moeckli 2016).

150 See the ECtHR judgment Appleby and others v. United Kingdom (2003) Application no. 44306/98, concerning the freedom of expression (Art. 10 ECHR) in which the Court observed: 'While it is true that demographic, social, economic and technological developments are changing the ways in which people move around and come into contact with each other, the Court is not persuaded that this requires the automatic creation of rights of entry to private property, or even, necessarily, to all publicly owned property (government offices and ministries, for instance)' (para. 47).

'personal space' that people carry with them when moving around. With the proliferation of security measures, including digital surveillance technologies, in public space, parts of our private life that take place in public space are becoming endangered. Moreover, as public space is becoming an increasingly *controlled* and *secured* space, the room for a healthy level of disorder and difference is disappearing. As many scholars – coming from political theory as well as psychology and sociology – have shown, this layer of disorder is not only desirable in order to enable and preserve the sociability and community in the city, but also in order to enable a more trusting, peaceful and (agonistically) democratic living together. Public space is, and should be, both space of order as well as space of disorder. Regulators should take notice of this and provide for limits to the increasing purification of public space, which should also lead to increased protection of privacy in public, creating a more desired balance between publicness and privateness. These arguments are strengthened by another insight from geography, namely the role of place in identity building.

5. PUBLIC SPACE AND ITS EFFECT ON IDENTITY BUILDING: A PHENOMENOLOGICAL PERSPECTIVE

5.1 Place and identity

The issue of place and identity, refers to the question of how people construct and enact their identities in spatial settings. Places 'are fundamental in expressing a sense of belonging for those who live in them, and are seen as providing a locus for identity' (Hubbard & Kitchin, 2011, p. 6). Given that identity is often formed through narratives (Somers, 1994), making sense of ourselves involves mapping the world in which we live. Narration is, thus, a form of mapping, through which we try to re-establish our sense of place in the world (Tally, 2013, p. 46).

Thus, place and identity (self or, better, selves) are closely intertwined in a process of co-production (Entrikin, 2002). The idea that public space is important for identity formation is well recognised in human geography (e.g. Massey, 1994). Geographers, drawing from other disciplines, have analysed and theorised both, how the construction of identity is influenced by spatial constraints, and how it affects the construction of place. They have conceptually articulated these relations between place and identity under different terms: sense of place, topophilia, insideness, and rootedness (Antonsich, 2010). This has been explored particularly in relation to issues

of culture, race, and gender.[151] More generally, psychologists have theorised how the physical world participates in the socialisation of the self through the concept of 'place-identity' (Proshansky, Fabian, & Kaminoff, 2014). Place-identity is defined as a sub-structure of the self-identity, consisting of (broadly conceived) cognitions about the physical world in which the individual lives. These cognitions represent the 'environmental past' of the person made of memories, ideas, feelings, attitudes, values, preferences, meaning, and conceptions of behaviour and experience, which relate to the variety and complexity of physical settings that define a person's day-to-day existence (*ibid*., p. 77). As such, place-identity is an individual's strong emotional attachment to particular places or settings.

The fact that individuals indeed define – at least to a certain extent – who and what they are in terms of strong affective ties to the home, the neighbourhood and the community, has been confirmed by both geographers and philosophers. Geography has engaged with conceptualising the home as the primary place where identity may be formed. 'Home is where you can be yourself. In this sense home acts as a kind of metaphor for place in general' (Cresswell, 2015, p. 39). The home can also be connected to Heidegger's notion of 'dwelling as the ideal kind of authentic existence' (Cresswell, 2015, p. 39; Heidegger, 1971) and seen as a place of intimate human relationships, family life, and care for the sick and injured (Tuan, 2001, pp. 137–138). Bachelard's (2014, p. 4) conception of the home as a place of 'attachment that is native in some way to the primary function of inhabiting', arguing that this is formed through images and memories, also intrinsically connects the home to identity construction. Notably, the (house as) home is a historically contingent form of social organisation, having evolved over the past centuries particularly as a construction to house the nuclear family; through social changes in households, its function and shape are now shifting (Madanipour, 2003, p. 106). Indeed, the home is not an independent space:

151 Cultural identity is socially and spatially constructed, in a process of co-production. Jackson has for example analysed how 'subcultural groups fashion identity through appropriation and transformation' of artefacts. Through a geography of cultural materialism, cultures can be studied as 'maps of meaning through which the world is made intelligible' (Jackson 1989; emphasis in original; as quoted in Hubbard & Kitchin, 2011, p. 259). In a similar vein, Butler's work on gender and identity has influenced geographers' study of identities and bodies in relation to their spatiality, for example inspiring studies that argue 'that bodily performances [such as the Rio Carnival] themselves constitute or (re)produce space' (*ibid*., p. 86). Scholars such as Sibley (1988), in psychoanalytically informed studies of self-construction, argue that boundary management of the self may also be connected to a deeply engrained desire for cleanliness and purity, leading to marginalising minority groups as 'polluting' the environment and the 'purification of social space'. This also connects to for instance Jackson's (1989) work on patterns of social interaction, segregation, and ghettoization.

it takes meaning only through the spaces it is not—the home is 'co-constituted as home by encountering an alienworld' (Steinbock, 1995, p. 182). Moreover, several feminists have contested the 'rosy view of home' and argued it to be a central site of oppression of women (e.g. MacKinnon 1989), although others emphasise the home's relative freedom from oppression that marginalised groups, such as black people, suffer outside (Cresswell, 2015, pp. 40–41). The home is thus 'a particular kind of safe place where (some) people are relatively free to forge their own identities' (*ibid*., p. 41).

Furthermore, citizenship – as a part of our identity that is essential for democracy and the political public sphere in general – is also partially developed as a spatial issue. This is so because we are not born citizens, rather, we must develop the behaviours and attitudes necessary for citizenship. As Jacobson (2010, p. 219) put it:

> 'We develop into a public being, that is a citizen – able to act as an independent and self-controlled agent in a community of similarly independent and self-controlled agents, especially in a shared space –, only by emerging from our familiar, personal territories – our homes.'

Only on the basis of a secured sense of ourselves and what is 'ours' (which develops in relation to the home) do we have an anchoring point that allows us to navigate among the multitude of places, things, customs, people and so on, that are not familiar to us (*ibid*., p. 223). The home thus provides us with a stabilizing and centralizing force. This means that leaving home is essential to our experience of home *as* home. In this sense, public spaces can be defined as those in which we explicitly or implicitly feel ourselves to be stepping outside of 'our own' ways and into ways of 'the world' – ways of being in which we may cooperate but that are not and cannot be 'ours' in a private or home-like way (even when we are comfortable in them) (Jacobson, 2010, pp. 330-1; see ref. 36).

However, also public places can have a similar same function, especially in light of increasing mobility and what geographers tend to refer to as 'time-space compression' – the processes by which distances are crossed more rapidly by people, goods or information (Warf, 2011, p. 144; see Section 5.2 on Technology and space). McLuhan (1994, p. 5), for instance, gave particular importance to the electronic media, famously stating that the world has become so compressed and electrically contracted, so that 'the globe is no more than one village'. While this statement is clearly an exaggeration, it does show the socio-economic and technological developments, including air travel and the internet, through which distant places are discursively repositioned as 'not that far away after all' (Warf, 2011, p. 147). In this sense, previously-far-away-places

that are now relatively close (distances between cities are now more often given in terms of hours rather than kilometres) also seem less foreign and thus less dangerous; furthermore, they become possible places, which can take part in the formation of our identity. One can now relatively easily and often travel to traditionally far-away places (at least from the perspective of a European), such as Taipei (about 12h *away* from Amsterdam), making it possible to develop a sense of familiarity with the place, thus developing 'a sense of place' on the streets of Taipei.

Although the home may still be seen as a key place where identity can be constructed, with time-space compression and increased mobility, the experience of place may still be rooted and localized, but in much more fluid, diverse, and networked ways than being attached to a single place of dwelling. The narratives people use to understand themselves in the world, which are constitutive of their identity, are nowadays associated with multiple places and flows, and thus equally formed through people's experiences in public places as they are through living at home.

Public space is also important to the construction of group identities. Social groups, just as individual persons, do not exist *a priori*, rather public spaces of the city (more so than other spaces) have a great impact on group identity formation (Ruddick, 1996). Moreover, it is the interactions that occur – that can and may occur – in public space that are crucial for the formation of various social identities. This is so because public space is not an inert environment for expressing fixed social behaviours, rather it is a medium for constructing new class cultures (Berman, 2006; Zukin, 1995), sexual and gendered identities (Wilson, 1996) or the places where marginalized identities can be challenged or confirmed (Ruddick, 1996). New social identities and meanings of public space are, hence, constructed together.

5.2 Technology and space: mobility, time-space compression and hybrid spaces

The increasing mobility of people, things, and capital in the past decades, and the associated process of globalization, have an obvious impact on space and place. The blurring and collapsing of spatial barriers, through for instance air travel, telecommunications, and the internet, are transforming our experience of space (May & Thrift, 2001; Tally, 2013, p. 41). Thus, Castells (2000) has argued, in the network society, the traditional 'space of places' has given way to a 'space of flows', where the creation of places becomes more dynamic than envisioned in Tuan's emphasis on *stasis* (see Section 2.1). The implications of this are manifold. Some have highlighted, for example, how globalization, privatisation and securitisation (see Sections 4.2 and 4.1) involves the creation of 'non-places': fleeting sites where history and tradition

are irrelevant, such as highways, airports, and supermarkets (Augé, 2009, p. 78). This requires thinking of space and place not in terms of boundaries and roots but from the perspective of movement and routes (Cresswell, 2015, p. 78). This implies that identities can – and need to – be construed 'in cosmopolitan forms of mobility rather than in stable and bounded places' (*ibid*., p. 81). Bauman (1998) argues that globalization and deterritorialization go together with reterritorialization of the nation-state – thus, 'glocalization' – but that the resulting social change empowers the privileged globals with freedom of movement and disempowers the static locals. All of this shows the on-going importance of space and place also in a globalizing world.

Others have debated the implications of the time-space compression that results from mobility and globalization enabled by technological development. Time-space compression, also called the 'shrinkage' or 'collapse of space' (Harvey, 1996, p. 240), generally refers to the set of processes that cause the relative distances between places (i.e., as measured in terms of travel time or cost) to contract, effectively making such places grow 'closer.'[152] Cresswell (2015, pp. 88–114) contrasts Harvey's and Massey's analyses of how people re-invent place in a globalizing world. Harvey (1996) emphasises the power-play and conservatism in people's efforts to re-create a sense of place to resist the forces of global capitalism and migration, showing how dominant groups in gated communities monopolise the meaning attached to a local neighbourhood to the exclusion of 'others'. Massey (1994, p. 151) agrees that the desire for rootedness and creating a sense of place to provide stability in a moving world can be reactionary and 'a form of romanticized escapism', but argues that this does not have to be the case. Time-space compression does not necessarily lead to feelings of insecurity but can also lead to a 'progressive concept of place'. This is characterised by place as process, involving multiple and diverse identities, defined by interactions with the outside rather than by an intrinsic unitary identity associated with the place. Places therefore are not settled, but continuously demand negotiation with the 'throwntogetherness' that characterises today's places in a progressive reading (*ibid*., pp. 141-156). Yet, people seek and experience rootedness and boundaries in relation to the outside and to diversity in different, complicated ways. What is clear, in any case, is that place is nowadays less associated with a particular location where people feel rooted. McCullough (2006, p. 29) captures this eloquently:

152 Warf, B. (2017). Time-space compression. Retrieved March 22, 2019, from http://www.oxfordbibliographies.com/view/document/obo-9780199874002/obo-9780199874002-0025.xml.

> 'At least to the more mobile and networked of us, place has become less about our origins on some singular piece of blood soil, and more about forming connections with the many sites in our lives. Place [has] become less an absolute location […] and more a relative state of mind that one gets into by playing one's boundaries and networks.'

McCullough ties in to another strand in the time-space compression debate: the role of the internet and new media. In its early days, the internet was conceptualized as a separate, online space existing in parallel to the offline world (see Kitchin & Dodge, 2011). A common claim was that virtual communities and the development of new forms of digital public spaces have facilitated the demise of 'real' material public spaces (e.g. Aurigi & De Cindio, 2008; Mitchell, 2003). On the contrary, scholars are now emphasizing the enmeshing of the virtual and the physical environment (J. E. Cohen, 2007; Crang & Graham, 2007; Kitchin & Dodge, 2011). 'As virtual [environments] and the "real" world have become ever-more tightly interwoven, digital networks have exerted a rapidly increasing influence over the social fabric, to the point where distinguishing between these two domains no longer seems helpful' (Warf, 2011, p. 148).

In line with McCullough's arguments above, Willis (2016, p. 160) discusses the capability of wireless communication technologies, such as wifi to enable 'multiple social realities' to occur in a single place. A person can thus be engaged in a politically charged debate on social media while at the same time having a beer and a face-to-face conversation in a pub (although the other person involved in the conversation might be very much annoyed by the constant typing on the phone). ICTs – both those embedded in public space as well as those carried by individuals – lead to a complex layering of public space that is 'multiplexed and overlaid', making it possible to easily switch from one activity to the next while remaining in the same physical space (*ibid*., p. 160). Public space is thus a site of multiple interactions (public and private), complex layering and visible as well as invisible interactions (de Freitas, 2010, p. 634). This leads to a high level of interconnectedness and interoperability, resulting in the absence of clear boundaries of public spaces (Mc Mahon & Aiken, 2014).

Furthermore, locative media, such as GPS-equipped devices and geo-location-based services, alter our relationship with and experience of place. Through these media 'the physical, tangible world combines with virtually accessible information and creates not a fixed setting for interaction, but a lived, fluid, and subjective space, shaped by space, time, and information' (Zook & Graham, 2007, p. 468). However, as our attention in space is focused through digital media-filtered information rather than through physical cues in urban landscapes and architecture, the addition of

location-based information alters our experience of place. The filtering, for instance in Google Maps, depends on economic and political interests, but this is not visible to most (non-critical) users who take location-based information at face value. And this 'lack of visibility in software can easily translate into a lack of visibility in hard-where (place)' (*ibid*., p. 468).

Relatively new notions, such as 'hybrid space' (Kluitenberg, 2006), might be useful for 'beginning to come to terms with the complex relationships between information, technology, society and space' (de Freitas, 2010, p. 631). Hybrid spaces are the result of intersecting digital and material spaces. They are spaces 'in which the public is reconfigured by a multitude of media and communication networks interwoven into the social and political functions of space' (Kluitenberg, 2006, p. 8). In contrast to Castells' spaces of flows, which can in principle lack any physical location whatsoever, hybrid spaces – although potentially global in scope – will always be rooted in local networks and connected to a distinct local history (de Freitas, 2010, p. 636). Sassen (2006, p. 23; as quoted in Crang & Graham, 2007, p. 790) similarly posits that global digital networks and transnational flows are deeply embedded in ways that mean that many 'urban residents begin to experience the "local" as a type of microenvironment with global span'.

Hybrid places, however, also produce new patterns of identification and stratification in place. In fact, Crang and Graham (2007, p. 791) posit that in such places, the identification and locating of people becomes a key issue. Far from the anonymity (or obscurity) of urban places past, hybrid urban places of the present enable hyper-visibility. Following De Certeau (1988), one might also call them 'readable spaces'. The following question is what are the implications for people in such places, that is, networked environments where small informational devices and data are brought together – repeatedly, sometimes in real-time time and automatically, through systems that are hidden in the urban background (Crang & Graham, 2007, p. 790)?

6. CONCLUSION

Following multiple perspectives on public space, including a socio-spatial, political and ontological perspective, informed by insights from geography and other relevant fields of research, I have examined concepts such as space and place, the public/private distinction, and issues of power, identity and digital technologies in relation to public space. It is thus fair to say that this Chapter is dense and packed with insights. However, there are a few key insights that need to be taken from this Chapter and

that will form a key part of the context within which I will discuss and conceptualise privacy in public space in the following chapters, particularly Chapter 7. I recap these in a condensed and simplified manner below.

The first key insight relates to the fact that public space is important for two general reasons: first, because it provides a physical space for interpersonal communication and social encounters that make a community possible (I have termed this 'sociability') and, second, because it represents the stage where – visible to others – individuals, groups, and crowds become political subjects. However, in relation to both of these functions, a special type of visibility is at play. In relation to political participation, Arendt's notion of the mask is important. Such a mask (today often referred to as anonymity) allows for a person's voice to be heard, while hiding individuals' (*idem*) identity in order to protect them from interference of powerful actors, both public and private, as well as peer pressure. Similarly, in order for public space to function as a space of sociability, encouraging mingling and interaction between strangers of various classes, races and ages, 'social distance' is needed. Such social distance is based on social norms and conventions (including civil inattention and reserve), which is connected to the transformation of public *space* into public *place*, an environment in which social trust exists or is at least possible. Without such trust, a community cannot emerge. Therefore, public space is not only as a space exposure, it is also a space of obscurity or inconspicuousness. However, in view of technological developments, these layers of obscurity and inconspicuousness in public space are at risk, thus endangering its two key functions.

The second key insight is that the public and the private exist in a complex and interrelated relationship. Unlike legal and many privacy scholars, geographers and political theorists have concluded a while back that public and private are inherently complex and unstable cultural categories that are mutually constructed. Therefore, the public sphere is not only a space of politics or sociability, it is also a space that is constituted in and through privacy. One needs a time and space for herself (often at home, in one's room), in order to develop her thoughts, opinions and identities before she can venture outside. Yet, if there is no public space into which one can venture and participate in the various activities of politics and sociability, an individual cannot fully develop into a citizen or community member and, thus, her personal development (her 'privacy') is limited as well. As such, public space should be seen as 'layered space', including many layers of private, semi-private, semi-public and public spheres (referring to spaces, persons, and activities; see also Koops, 2018). This means that not only are public and private not binary oppositions, they go hand in hand. As Warner (2002, p. 27, 30; as quoted in Iveson, 2007, p. 9) put it: 'Public and private are

not always simple enough that one could code them on a map with different colors – pink for private and blue for public . . . [M]ost things are private in one sense and public in another.' This applies to streets and homes as much as it applies to places that are more obviously hybrids of public and private, such as shopping malls and public toilets. Any 'where' is thus potentially the context for combinations of both 'public' and 'private' action (Iveson, 2007, p. 9).

Finally, the last key insight relates to the idea that public space is important to the construction of our identities, both individual and collective, providing a *locus* for identity. This is thus a function that public space shares with privacy (see Chapter 3). Identity, both individual and social (which are thoroughly interrelated), is nowadays conceptualised as a process (rather than as a fixed thing; see Jenkins, 2014). Not only is public space important to the construction of individual identity, especially in relation to becoming a fully-formed citizen, it is also important for the construction of group identities and communities. Social groups (as well as individuals), namely, do not exist *a priori*. In particular, it is the interactions that can and may occur in public space that are crucial for the formation of various social identities. As people build their identities in relation to places, particularly places where they feel at home or 'in place', identity and place construction need to be considered jointly as being co-produced. This suggests that privacy as the freedom (or breathing room) to define and re-define oneself as a subject (which is how I understand the concept of privacy; see Chapter 3) should be analysed in relation to place in all the richness, variation, and complexity that place entails, which goes far beyond a simplistic notion of a 'private place', epitomized by the home, that, in a legal and regulatory context, is all too often associated with privacy. Identities connected to being-at-home are also constructed in public places, in movement, and in physical-digital networked spaces.

However, with the privatisation and securitisation of public space (including within the development of cities into smart cities and living labs), social action is becoming increasingly tightly scripted and prescribed. Such control of public space is said to be based on a reconfiguration of liberty that excludes many non-criminal conducts, activities, groups and even political practices, and is heavily based on preconceptions, prejudices, and fear of potential harm rather than real danger. This can not only lead to discrimination and exclusion of certain groups (and domination of others), it can also have important consequences for identity formation, including autonomy. The mobile nature of identity construction in a space of flows suggests that privacy, as freedom to shape one's identity, also requires protection in public. Moreover, the enmeshing of virtual and physical space implies a need to reflect on how the embodied experience of place is influenced by digital information flows projected

onto and interacting with physical space. What kind and level of protection that should be, depends on concrete situations and contexts – one cannot give generalized rules for 'privacy in public space'. While this challenge is starting to be taken up (e.g. J. E. Cohen, 2012), it requires considerable further study, not least in relation to concrete places and practices. Taking up this challenge, I thus discuss the types and characteristics of surveillance within the example of the *Stratumseind Living Lab* and the particular privacy-related risks stemming from them in the following Chapter.


De Bakker
Big Brother
The Orwe
vermogen
vervuiler
muziek-
smaak
Schilderswijk
politieke
voorkeur
adres
wijk
functie
adres
digibeet
IQ
pedofiel
hoog-
opgeleid
cultuur
smaak
racist
potten-
bakker
provincie

PART II

5

SURVEILLANCE *IN* AND *THROUGH* PUBLIC SPACE

Surveillance within the *Stratumseind Living Lab* and privacy-related risks

1. INTRODUCTION

The expansion of surveillance within smart cities – and its implications for privacy – has been largely overlooked, especially when compared with the scholarly attention that CCTV (closed-circuit television) received at the end of the 1990s and in the early 2000s (Bannister, Fyfe, & Kearns, 1998; Doyle, Lippert, & Lyon, 2012; Fyfe & Bannister, 1998; Norris, 2003; Norris & Armstrong, 1999).[153] While smart cities and similar innovation platforms, such as living labs, have been extensively debated from the perspective of urban geography (thus pointing out numerous perils, including ideological rhetoric, a technocratic form of city governance and the transformation of public space into quasi-public space; see Chapter 1), an equally thorough investigation has occurred neither in surveillance studies nor in privacy theory literature. This Chapter addresses this omission by examining the *Stratumseind Living Lab* from the perspective of surveillance studies and privacy theory.

It is not uncommon today for smart cities to be called 'surveillance cities' or something of the sort (Lyon, 2018; Monahan, 2018; Murakami Wood, 2015; Sadowski & Pasquale, 2015). Scholars have expressed smart city concerns about individual's privacy, autonomy, freedom of choice, and discrimination (Finch & Tene, 2018). However, questions of what exactly does this mean, in which cases do these issues arise, how and for whom often remain unanswered. Likely stemming from critical research on CCTV (e.g. Davis, 2006; Fyfe & Bannister, 1998; Norris, 2003), many scholars employ the old-fashioned Panopticon or Big Brother metaphor for the type of surveillance found in smart cities (see e.g. Finch & Tene, 2018; Kitchin, 2014). They do so despite the common criticism that these metaphors are out of date (see Chapter 2). The choice of theoretical framework through which one analyses contemporary surveillance practices within smart cities is important, as it can have detrimental (or beneficial, for that matter) consequences for what one can (and will) conclude, including in terms of its risks. Is it therefore enough to state that 'smart city privacy issues reflect traditional concerns about the panoptic gaze of a surveillance society' (Finch & Tene, 2016, p. 1594)? I argue that it is not.

The thematic-historical examination of surveillance theory in Chapter 2 shows that contemporary networked surveillance practices are much more diverse and complex than a panoptic gaze. They also transcend the public-private divide. Surveillance is carried out by both public and private actors (including individuals), increasingly in

153 With notable exceptions, such as: Monahan (2018); Murakami Wood (2015); Edwards (2016); Sadowski and Pasquale (2015).

complex public-private partnerships, for public (that is common) and private purposes, for control and care, over suspects and non-suspects, and within public, semi-public and private spaces. These surveillance practices often support each other in a complex manner that is almost impossible to disentangle. Surveillance thus needs to be understood and examined in its aggregated and complex social context (Richards, 2013, p. 1935).

The risks for privacy stemming from such surveillance practices need to be examined in such a manner, as well. I use 'risk' here as it is used in everyday language, associated to the idea of potential future danger, that is, 'an eventual danger that can be foreseen only to some extent' (Godard, Henry, Lagadec, & Michel-Kerjan, 2002, p. 12). Yet, surveillance scholars (and sometimes legal or policy scholars) commonly differentiate between 'privacy' and 'non-privacy' risks, wrongs, dangers, harms or however authors might refer to them (e.g. Gilliom, 2006; Macnish, 2018; similarly Wright & Raab, 2014; Lyon 2001). On the one hand, we have risks for privacy and, on the other, we have other types of risks, such as chilling effects, diminishing trust, issues related to power and control, social sorting, exclusion from public space, and problems with errors and false positives (Macnish, 2018, p. 31). According to Möllers & Hälterlein (2013, p. 57) privacy as a defining theme in surveillance research has been widely rejected 'because it is regarded as too narrow to grasp the entirety of the social consequences resulting from surveillance practices.' In particular, several scholars base this 'rejection' of privacy on the limitations of 'the right to privacy', often not specifying which right they have in mind or referring only to data protection rights (e.g. Gilliom, 2006; Schermer, 2011; Wright & Raab, 2014). Moreover, journalistic and lay discussions of surveillance are almost universally framed around issues of data protection law, commonly referred to as 'privacy' (e.g. Kanters, 2014; Möllers & Hälterlein, 2013; Naafs, 2018).

While surveillance indeed has implications that go beyond privacy (particularly as discussed by urban geographers), this 'rejection' of privacy seems to stem from a reductive understanding of privacy, perceived as a rather straightforward and static term or a specific narrowly understood right. However, as privacy literature keeps on stressing, privacy is a very complex issue and should not be reduced to (control of) personal data (Koops et al., 2017). It is a very broad concept, the value of which stretches from the development of identity and autonomy to the formation of social relations and requirements for democracy (see Chapter 3). Privacy is thus not only an individual but also a social value, with numerous scholars expanding on the relationship between privacy and trust (Keymolen, 2016; Richards & Hartzog, 2016; Waldman, 2018) and the connections between autonomy or identity-development and conforming effects, social sorting and exclusion (J. E. Cohen, 2017; Kaminski &

Witnov, 2015; Nissenbaum, 2010; Solove, 2008; von Hirsch & Shearing, 2016). As I have concluded in Chapter 3, privacy has an 'infrastructural character': on the one hand, it is an important presupposition for autonomy, self-development, and other values that privacy contributes to; and, on the other hand, it is because privacy can serve many other values that it is also a value in itself (Koops, 2018). Understood in this way, it becomes clear that surveillance and privacy denote modes of ordering that are to a great extent orthogonal to one another and that they will enter into conflict both practically and politically (J. E. Cohen, 2017, p. 458).

There seems to still be a disconnect between surveillance theory and privacy theory. Understood in the above broad way, however, privacy fulfils an essential function that the view from surveillance studies risks overlooking. Consequently, I do not employ the privacy v. non-privacy risks distinction. Instead, I will refer to 'privacy-related risks', which can encompass many of the above-mentioned risks of surveillance, such as social sorting, chilling effects, group profiling, and exclusion. In this Chapter I do not perform a comprehensive overview of all privacy-related risks of surveillance within smart cities, as that would be a daunting task. Rather, I limit my analysis to the main types of privacy-related risks stemming from surveillance of public space within smart city developments: risks for identity, autonomy, trust, stigmatisation, sociability and political participation. In line with the focus of this dissertation, I intentionally leave out risks relating specifically to informational privacy, which are the primary concern of data protection law.

Following Solove (2008, p. 40), I employ an approach from pragmatic philosophy, according to which privacy issues should be worked out contextually rather than in the abstract. This is a particularly suitable approach for the focus of this dissertation, that is, privacy in public space in the context of smart cities and living labs. While smart cities and living labs come in all shapes and sizes, I use the example of the *Stratumseind Living Lab* (*SLL* or *Living Lab*) (in particular the *CityPulse*, *De-escalate* and *Trillion* sub-projects) in order to determine the particular types of surveillance taking place within it and the risks that they pose for privacy (understood in the above broad manner). In this Chapter, I thus answer the sub-question: *which types of surveillance and their characteristics are found operating within the Stratumseind Living Lab and what are the privacy-related risks stemming from them*?

This example comes with its own limitations. As already explained in the Introduction of this dissertation, I employ the *SLL* as an illustrative example of a living lab (and a part of a broader smart city development of the city of Eindhoven) focused on safety and profitability (see Chapter 1). As such, insights based on this example are not

(necessarily) valid for other types of living lab or smart city initiatives with other foci. In order to go beyond the particularity of this example (and also in view of a lack of detailed information on the functioning of the *SLL*), I employ hypothetical scenarios. Some of the scenarios that I use (presented in distinct text boxes) are closely based on the shared information on the workings of the *Living Lab*, while others are more speculative (but not unimaginable given the types and characteristics of surveillance within the three examined sub-projects). Scenarios are a type of story-telling with a specific purpose (Wright, Gutworth, Friedewald, Vildjiounaite, & Punie, 2008, p. 21). In this Chapter, they allow me to analyse potential privacy-related risks connected to smart city/living labs surveillance, going beyond the concrete successes and failures of the *Stratumseind Living Lab*. They are also expected to stimulate discussion in this area of research that has not gained sufficient attention. Finally, the results of such analysis and discussion may be used in preparing 'roadmaps (how do we get from here to the future we want) and setting strategic research agendas (what must be developed)' (*ibid*.), which I try to do in Chapter 7.

2. AN ANALYSIS OF SURVEILLANCE PRACTICES WITHIN THE *STRATUMSEIND LIVING LAB* FROM SURVEILLANCE STUDIES AND PRIVACY THEORY PERSPECTIVES

In order to identify the characteristics of surveillance practices within the *SLL* and the types of surveillant logics they represent, the analysis in this Chapter will follow the five broad themes identified in Chapter 2 on surveillance theory. These main themes can be summed up in the following questions:

(1) Is surveillance physical, confined and stable or numerical, networked, open (or liquid) and invisible?
(2) Who are the main actors of the surveillance?
(3) Who is the subject of the surveillance and what is its focus?
(4) What is the aim of the surveillance?
(5) Is surveillance perceived as negative and sinister or positive and even empowering

I will further inform the discussion through insights gained from Chapter 3 on privacy theory by identifying specific privacy-related risks stemming from specific surveillance practices within the *SLL* sub-projects. I will do this by employing hypothetical scenarios, so that I can determine with a level of concreteness (although remaining speculative), whether the surveillance practices connected to the *SLL* pose privacy-related risks and, if so, which risks in particular, and in which ways.

Figure 5.1: CityBeacon *on the Stratumseind street (photo taken by author, 26 August 2018)*

2.1 Sensor-based surveillance: networked, open and largely invisible

The first characteristic concerns the question, whether surveillance is physical, confined and stable, or numerical, networked, open (or liquid) and invisible. Since surveillance within the *SLL* concerns mainly surveillance of physical public space, it is to a certain extent physical and confined to the Stratumseind street. Nevertheless, as it is performed through an increasing number and type of digital technologies operating as sensors (first via video cameras with embedded capabilities, later adding sound cameras and dynamic lighting technologies), possibly spreading to other streets in the city[154] and relying on data capture and analysis, surveillance is also – and predominantly – networked, open and invisible. The opaqueness of such surveillance is enhanced as sensors and the computer-communication systems that support them are becoming embedded in the urban environment and thus less noticeable for the passer-by. This is, of course, not equally true for all of the types of surveillance technologies within the *SLL*. *City Beacons*, on the one hand, are large conspicuous structures that stand on the side of the street and can hardly be missed (although their diverse surveillant capabilities are not at all clear). On the other hand, sound cameras and WIFI tracking technologies, often in the shape of little black boxes mounted on classical street lighting are not very distinctive and visible. Furthermore, throughout the operation of the *SLL* (2013-2018) no sign notifying of the surveillance has been placed at the entrances to the Stratumseind street.[155]

154 During the period of operation of the *SLL* (2014-2018) some technologies that were first introduced on the Stratumseind street were then introduced on other streets in the centre of Eindhoven (based on my interviews with the actors of the *SLL*).

155 Last checked by the author on 15 October 2018.

Figure 5.2: *Video camera, sound sensors, special lighting technology, wifi tracking technology and possibly other surveillance technologies in front of the Sint-Catharinakerk close to the main entrance to the Stratumseind street (photo taken by author, 26 August 2018)*

Many sensors are embedded in the fabric of the Stratumseind street (e.g. attached to buildings or existing lighting poles) for the purpose of *direct* sensing, including 'smart' video cameras, sound sensors and sound cameras, a weather station and *iBeacon* technology. *Indirect* sensing is also taking place within the *Living Lab*. This type of sensing uses interactive, networked devices and applications, most notably smart phones, that come to double as sensors (Andrejevic & Burdon, 2015, p. 20). In this sense, the smart phone (with GPS technology) can function as a tracking device. In fact, any networked interactive device can double as a sensor insofar as it collects and shares data about its use; this data can then be used to infer information about the user and the user's environment (*ibid*., p. 21). In the case of the *SLL*, smart phones are used to determine the residence and nationality (as is discernible from the residence and mobile subscription) of the visitors of Stratumseind. Their smartphone's unique identifiers, although pseudonymised, are also caught by the WIFI tracking performed by *SLL*. The surveillance within the *SLL* is thus predominantly 'sensor surveillance', representing a pervasive, always-on and passive type of data collection (*ibid*., p. 20).
The *SLL* not only monitors physical public space of the Stratumseind street and its surroundings, it also monitors – although to a much lesser extent – certain social media, such as *Twitter*. It performs a simple type of sentiment analysis by analysing tweets that are somehow connected to Stratumseind (e.g. naming the street, a certain

bar on the street or a particular well-known bartender) and classifying them as positive, negative and neutral. In this sense, the public – visitors of Stratumseind – are willingly exposing themselves and thus participating in their own surveillance. However, while this might indeed be a dominant mode of surveillance within certain contexts (such as in relation to social media in general), it plays only a minor role within the *SLL*. According to the *SLL* project manager, the visitors of Stratumseind do not tweet too much about the nightlife on the street – there are usually between 25 and 50 tweets on a busy Saturday night and most of these are considered neutral by the sentiment analysis performed. In other words, the tweets do not reveal much about the perception of the activity or atmosphere on the street (either positive or negative), rather they mostly share information about nearby events on the streets or in the pubs. While performing sentiment analysis was planned also in relation to Facebook-data, this idea did not materialise within the projects (likely because of data

Figure 5.3: *A tweet suggesting positive atmosphere ('lekker sfeertje') on the Stratumseind street*

protection law considerations). The *SLL* surveillance practices are thus not particularly focused on social media.

However, developments in the direction of more social media surveillance (or other directions) are not unlikely. Networked technologies namely display the dynamics of surveillance creep – the process whereby surveillance measures (both low- and high-tech) introduced for one purpose can quickly develop new uses, expanding the focus on new places and populations (Haggerty, 2014, p. 236). As Haggerty (*ibid.*, p. 241) points out, in many contexts the spread of video surveillance in cities represents a clear example of surveillance creep. While most cameras were initially justified as a means

to counter high-level crimes such as child abduction and terrorism,[156] once installed, authorities began to use them to address a host of low-level regulatory matters and monitor the minutiae of public behaviour. In the UK, for instance, local authorities have used cameras largely deployed for terrorism purposes to regulate people putting their garbage out on the wrong day, not cleaning up after their dog, urinating in public, littering, smoking under age and posting flyers (*ibid*.). We cannot speak of the *SLL* sub-projects in the same way, as technologies there were being developed 'on the street itself' for the particular purposes of the Stratumseind street.[157] Nevertheless, it is not unimaginable that these technologies developed for the particular purposes will not be repurposed in another way in the (near) future, especially in view of their limited successes in terms of their promises (particularly within the *CityPulse* and *De-escalate* sub-projects; see Chapter 1). This uncertainty potentially poses problems for the legitimacy and foreseeability of the purpose required for surveillance in public space.

This is further connected to the open-ended structure of surveillance within the *SLL*, which can be described as a surveillant assemblage (Haggerty & Ericson, 2000). The *SLL* namely consists of several projects, various types of technologies, actors, subjects, relations and goals of surveillance with a seemingly rhizomatic structure – like the roots and shoots of a persistent set of plants, it seems to pop up everywhere. As new goals were created and projects continued to evolve – some ending and new ones beginning – a complete overview of the structure was hardly possible, at least until the official end of the *Lab*. The *Stratumseind 2.0* and the *SLL* thus had no distinct boundaries, rather they remained fluid fields. Even now, after the official end of the *SLL*, similar or follow-up projects (with some of the same parties) might continue under different names.[158] Indeed, the inevitability of transformation is key to thinking in terms of assemblage. As such, surveillance within the *SLL* can be described as emergent, unstable, lacking discernible boundaries and even accountable actors, so

156 The demand for CCTV in the late 20th century in the UK, for instance, was closely connected to the public outrage over the tragic abduction and killing of a two-year-old toddler by two ten-year-old boys in 1993 (Norris, 2014).

157 Although, of course, concrete technological ideas were introduced by private companies offering their services to the municipality. For example, Vinotion had developed a people counting and anomaly detection in movement software, which it then offered for use (and further development, made easier through testing in a 'real-life' environment) to the *SLL*.

158 Indeed, a recent post on the 'Living Lab, Stratumseind 2.0' open Facebook group seems to suggest a continuation of work similar to the one in CityPulse with the company Vinotion; see Vinotion. (2019). Living Lab, Stratumseind 2.0. Retrieved March 27, 2019, from https://www.facebook.com/LivingLabStratumseind/.

that it cannot be criticised by focusing on a single institution. It is therefore important to deconstruct the surveillance within the *SLL* further in order to properly analyse and critique it.

2.2 Public, private and individual actors of surveillance: issues of trust and (re)stigmatisation

A multiplicity of actors can be observed within the *SLL*, which is organised in the form of a public-private partnership (PPP). Among the public actors, we find the municipality of Eindhoven, the local police and local public universities (such as Technical University Eindhoven and Tilburg University). Amid the private corporate actors, we find a large number of ICT companies, some big multinationals (such as IBM, Cisco, Intel, Philips, Atos and Vodafone) and others small and local (like Sorama, Vinotion and Mezuro). Alongside these companies, other minor private actors, such as breweries, pub owners and real-estate owners, are also involved.

It does not suffice to describe the type of surveillance that is being operated by or on behalf of these actors as 'classical' surveillance, where a top-down technique of power operates (similar to the surveillance operating within Bentham's prison Panopticon). Although that can also be observed. Within the *CityPulse* and *De-escalate* sub-projects, citizens are also surveilled by those with public authority – the municipality and the police. However, because the *SLL* projects operate within a PPP, much of the surveillance is in fact developed and performed by private companies on behalf of the public actors (although also for their own private goals; see Section 2.4). Within the *CityPulse* project, for example, private companies developed a physical aggression detection system (its prediction capabilities remain undeveloped, at least for now) for the municipality, which is responsible for the maintenance of public order. This system could then also be used by the police desiring a more efficient deployment of police officers. However, private actors also gain something from these surveillance practices – they gain valuable data sets based on the observed activity on this public street, which can not only be used in order to develop their own technological systems (then to be sold to cities around the world) but can also be sold on their own to other companies (or governments). In this sense, we can state that private companies within the *SLL* that are surveilling citizens on a public street are acting *as* actors with public authority (but without proper legitimate basis; see also Chapter 7).

However, there is also another type of surveillance – by another type of actor – taking place within the *SLL*. Within the *Trillion* sub-project, a type of community policing project, lateral (or horizontal) and participatory surveillance are employed. In this case, individuals are surveilling other individuals on the Stratumseind street; in other

words, the many are watching the many. A concerned visitor of the Stratumseind street can download the *Trillion* app on her phone, which allows her to send pictures or videos (including direct transmission of video through the app) of trouble and troublemakers to the local police. Individuals are thus variously involved, both watching and being watched through surveillance practices on the Stratumseind street.

The *Trillion* community policing project differs from classical neighbourhood watch schemes, which involve peer-to-peer surveillance practices initiated by groups of citizens themselves in order to counter criminal and undesirable behaviour and to improve the quality of life in their local area (Ball, 2019, p. 91). On the contrary, in *Trillion*, community policing is initiated by the municipality in collaboration with private companies and the police. It offers a ready-made platform for the participation between citizens and the police – that is, through the *Trillion* app. The types of events that can (and indeed should) be reported are given in advance (e.g. drunken behaviour, trash on the street, noise), although some freedom to report remains (one can choose 'other' type of event/issue to report). In doing so, the app developers (in collaboration with the municipality and the police) determine in advance which types of behaviour are acceptable and desired on the street and which are not. As such, the level of participation of citizens in the decision-making processes is limited, as they merely provide an image, video footage or a description of the reported event. In turn, this leads to 'artificial fitting' of observed behaviour into these predetermined categories, which is highly reductionist and can lead to interpretation bias (that is, finding what one is looking for; I discuss this further in the following sub-section, 2.2.1). These lateral surveillance practices can thus still be described (at least partially) as top-down, since individuals are largely representing 'eyes' on the street for the municipality and the police.

This type of organisation of lateral surveillance can also have a positive effect. While classical neighbourhood watch initiatives commonly use social media to share personal information, such as images of 'suspicious' persons or vans (and their license plates), with each other and the broader public, within the *Trillion* project this information is only shared directly with the police (unless, of course, the person also directly posts it online). In this sense, the *SLL* project diminishes potential privacy issues concerning the sharing of personal data with the general public. In Austria, for example, the police turned down on data protection grounds potentially useful personal data gathered by a watch group, because it was shared on social media (Ball, 2019, p. 100). The *Trillion* app can then be seen as a way of potentially overcoming certain data protection law issues.

Scenario 1:

It is a busy Saturday night out on the Stratumseind street. A group of four young males on the street are tipsy and talk loudly. They begin to interact with a group of girls there and one of the boys takes off 'cat ears' from one of the girls' head. The girls do not particularly like this and with a bit of effort snatch the cat ears back. Merel, a concerned citizen who has downloaded the *Trillion* app on her smartphone, is nearby and witnesses the exchange. She is alert and on the verge of making a video in order to report the nuisance via the app to the police. However, she interprets the event as 'playful' rather than as aggressive or 'macho behaviour' – she thinks to herself, 'boys will be boys', and leaves the phone in her pocket.

2.2.1 At the bottom of the participatory ladder: issues of trust, risks of over-reporting and (re)stigmatisation

There are, however, potential negative sides of such participatory lateral surveillance as well. As Albrechtslund and Lauritsen (2013) have pointed out, careful attention needs to be paid to the ways in which participation in surveillance is established, maintained and negotiated. There are many different types and levels of engagement in participatory practices, amounting to very different degrees of citizen power, which Arnstein (1969) conceptualised as the 'ladder of participation'. The question of participation in the community policing project on the Stratumseind street is particularly important in view of the culturally and ethnically diverse visitors of the nightlife street. As was noted by the projects actors themselves, a key issue in the *Trillion* project is trust between citizens and the police, which is needed in order for the app to be adopted in practice.

The issue of trust between law enforcement and citizens is, of course, a complex matter, highly dependent on context. In the particular context of trust between Dutch police and its multicultural and multi-ethnic inhabitants, certain minorities feel – sometimes rightly so – that they are unjustly targeted (see e.g. Eijkman, 2010).[159] Specifically in relation to Stratumseind, predetermined suspicion (partially based on police statistics) is found to be oriented against groups of young males, such as football fans and others exhibiting 'macho behaviour' (Kalinauskaitė et al., 2018). While 'macho behaviour' is, of course, not limited to a particular cultural or ethnic

159 See also: Pieters, J. (2016, May 31). Driving while black: rapper stopped by Zwolle police for pricey car. NL Times. Retrieved from https://nltimes.nl/2016/05/31/driving-black-rapper-stopped-zwolle-police-pricey-car/.

group, one can speculate that the underlying assumption in the case of the *SLL* is that such behaviour is more common amongst particular cultures, such as a particular Moroccan or Turkish Muslim culture.[160] In this sense, 'macho behaviour' can be (ab) used as a proxy for ethnic or racial discrimination. As such, certain groups are the object of heightened surveillance and, as can be expected, do not have a very high level of trust in the police (van der Leun, 2014). A further issue is whether these groups of citizens understand how to participate and become skilled in exercising civic rights and duties, and whether they even recognise themselves as citizens with rights that need to and *should* be exercised, which is to a large extent a product of class, gender, ethnicity, history and identity (Ball et al., 2019; Cornwall & Coelho, 2007).

It is thus not unlikely that the *Trillion* app would be mostly used by those groups (often white Dutch citizens like Merel in Scenario 1) that already have a sufficient level of trust in law enforcement and a distrust towards ethnic minorities. If we imagine Scenario 1 a bit differently, so that the rowdy boys snatching the cat ears would belong to a particular cultural or ethnic minority, Merel might interpret their behaviour in a different way – seeing it as 'macho behaviour' and potentially dangerous – and would report it to the police through the app. With the possibility to report any type of non-mainstream activity that an individual finds deviant (such as, drinking beer on a bench, smoking marihuana, talking loudly or even protesting), there is a higher risk of over-reporting and targeting certain groups. Such reporting, which is indirectly encouraged through the *Trillion* app, can thus serve as a cloak for prejudices against specific groups or individuals and can result in stigmatisation or re-stigmatisation of groups which are already disadvantaged (Ball, 2019, p. 95; Schermer, 2011, p. 47).[161] Therefore, the labelling of citizen-state interaction as 'participatory' may result in the marginalisation of certain voices and an overwhelming pressure to comply and consent to whatever state (or, increasingly, private) actors wish to accomplish (Arnstein, 1969). As Ball, Timan & Webster (2019, p. 28) nicely put it:

> 'Achieving participation goes way beyond merely inviting citizens to do so. It involves citizens seeing themselves as having a voice and being able to act meaningfully in those settings. If they have been subject to discriminatory state practices in the past, or are part of a marginalised group, this lens may come with them into the participatory space.'

160 This has been expressed during my interviews with the various parties to the project.

161 Examples of classical neighbourhood watch groups from Spain, Austria and Germany have been used by right-wing extremists and vigilante groups to propagate their beliefs about what is or is not acceptable behaviour or identity in a particular area (Ball, 2019, pp. 95–96).

This type of lateral surveillance thus might lead to increased scrutiny of minorities in public space (diminishing their possibilities to be inconspicuous – a type of privacy practice in public space), potentially furthering inequalities between different societal groups. The infrastructural character of privacy is clear here, where privacy is serving other values and goals – preventing racial discrimination, (re)stigmatisation and preserving trust.

2.3 Everyone under surveillance: security, control and risks for identity-development

Some of the data being captured within the *SLL* is focused on environmental and other non-human factors, such as weather data (wind speed, temperature, amount of rainfall), amount of trash generated on the street per week and amount of beer sold in the bars on the street per week. However, most of the data captured by the sensors on the street is focused on the daily activities of people there. Therefore, everyone that approaches or enters the Stratumseind street, either to simply pass by (as it is a street in the centre of town) or to visit a pub on the street, is surveilled. Everyone is caught by the video cameras and, if they make a loud enough sound, on the sound cameras. Persons' movements through the streets are captured. Unique identifiers of their mobile phones are also tracked through wifi tracking technology. Crowding levels on the streets (and possibly in particular bars) are determined. All of these data (including the data not focused on humans) are captured and analysed with the general goal of determining the 'atmosphere' on the street and influencing persons' behaviour (I discuss the goals of surveillance within the *SLL* in the next section). However, all of these surveillance practices are done in such a way that they do not *directly* identify any individuals (although individuals might still be indirectly identifiable, which I discuss below). For instance, faces on the video from the cameras are blurred and the unique identifiers of mobile phones are pseudonymised.

On the one hand, this approach to surveillance can be seen as a reaction to European data protection law, that is an attempt to avoid falling within its scope. At the beginning of the project, the actors within the *SLL* had claimed that they do not collect personal data, thus falling outside of the scope of data protection law. Several opinions of the Dutch data protection authority later (e.g. one which has declared almost all cases of video surveillance, including those with blurred faces, as collecting personal data),[162]

162 E.g. Autoriteit Persoonsgegevens. (2018). AP informeert branche over norm camera's in reclamezuilen. Retrieved March 27, 2019, from https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera's-reclamezuilen#subtopic-1727.

they have acknowledged that they do collect some personal data and have begun to take data protection law more seriously.[163]

On the other hand, this type of surveillance practice can also be seen as a development from a discipline-oriented surveillance to security-oriented surveillance. As I have discussed in Chapter 2, while the disciplinary way of governing people or activities consists of breaking down a given multiplicity into specific components, singling persons out and consequently identifying individuals (Foucault, 2007, pp. 55–56), security focuses on the relationships between components of a given reality, rather than on singularised entities separately (*ibid*., p. 47). From a security perspective, what matters is the optimised adjustment of the assembled components of reality depending on and in relation to each other (Klauser et al., 2014, p. 873). If discipline starts from a predefined optimal model that is rigidly applied to individuals (e.g. one must learn X in order to pass the test), the apparatus of security lets things happen within the limits of the acceptable, whilst also regulating and monitoring them with a view to the optimisation of reality in its intertwined components (*ibid*., p. 874). The logic here can be described as inclusionary and is thus involved in a constant process of optimisation derived from and taking place within a given reality, rather than postulating a perfect and final reality to be achieved.[164] Having settled on this perspective, I acknowledge the recent work of Ball (2009) and Ball, Di Domenico and Nunan (2016) who criticise the above Foucauldian treatment of surveillance, which assumes a direct gaze as its central feature, and instead suggest a focus on the notions of 'exposure' and 'intersecting proximities' between subjects and big data surveillance practices. These perspectives might offer additional insights in the matter at hand, calling for further research.

What does this mean in practice? It means that within the *SLL*, security is (ideally) sought through control without stopping or hampering the flow of visitors (their consumption) on the street. Persons are not surveilled and targeted individually, rather they are targeted *en masse*. The goal is not to identify every single breaking of the norm (in this case, every single type of anti-social or escalated behaviour) and intervene, for example by a pub's security guard or by the police, either in the form of a warning, exclusion from the pub, the street itself or arrest. The goal is to let

163 This information is based on my interviews with the manager of the *SLL* and DITTS. As data protection is not the perspective I take in this analysis (or the dissertation in general), I will not discuss this any further.

164 In this sense, Foucault's security is close to Deleuze's modulation, where systems or institutions are constantly changing and adapting within invisible networks.

smaller transgressions slide and try to manage their relationships with the whole – that is, try to not let them affect the atmosphere on the street – in such a way that an intervention will not be necessary. On the collective level, the *SLL* thus captures and analyses various types of data in order to produce risk categories in connection to the 'situation' on the street. The *CityPulse* system in particular categorises these risks in four general levels: (1) 'nothing wrong' situation; (2) 'everything alright' situation; (3) 'backup needed' situation; and (4) 'high risk' situation. While it is not at all clear, what is the difference between 'nothing wrong' and 'everything alright', one can assume that in these two cases there will be no *direct* intervention from the police (or security guards). Nevertheless, lighting and smell scenarios might still be turned on in order to de-escalate any mildly transgressive behaviour, which does not merit police intervention, and try to prevent it from happening in the future as well as affecting other persons' mood.

Scenario 2:

Imagine a couple, Freek and Marloes, who exhibit some type of mildly escalated behaviour. They are having a fight that gets out of hand, resulting in yelling and a broken glass or two. The *SLL* surveillance system captures the image and sound of them yelling and breaking glass and determines that this is a 'low risk' situation on the street (ie. 'everything alright'), turning on the special lighting and smell technologies. The lighting and the smell of oranges indeed help calm Freek and Marloes down, who make up and end up kissing in a secluded spot. Activity on the street continues almost undisturbed, Freek and Marloes are not individually identified and the surveillance likely does not directly affect them further (that is, beyond the nudging; discussed in the next section).

This fits rather well with the regulation of a nightlife street like Stratumseind, where a certain level of chaos (oftentimes due to intoxication) will always be present, as it is a part of the 'idea' of nightlife itself (Chatterton & Hollands, 2003). Research has shown that nightlife requires not only a sufficient level of safety but also a sufficient level of excitement and dangerousness, rather than completely predictable outcomes (Brands, Schwanen, & van Aalst, 2015; Timan, 2013). When the latter happens, people tend to move on to another, more exciting *nightscape*.[165]

165 The term nightscape refers to a specific time (the night) and place in the city understood as a landscape, which is made of both humans and things that behave differently at night than during the day (see Timan, 2013).

However, the *SLL* projects not only work on a collective but also on an individual level (Schuilenburg & Peeters, 2018). More specifically, the *SLL* operates partially according to a securitising logic and partially according to the exclusionary logic of control happening in invisible and opaque networks (following Deleuze).[166] The logic of control, however, not only kicks in when the securitising logic fails (e.g. in Scenario 2, when Marloes and Freek do not calm down and begin to physically fight so that city guards or the police need to be called); it also operates in parallel to it. Thieves and known troublemakers, for instance, are not desired on the street in the first place. Their presence on the street is not intended to be 'managed' through securitising logic, they are simply to be identified and excluded. While this might be desirable on a general level, as no one wants their purse stolen on a night out with friends or their friend assaulted by a bully, how these 'undesirables' are identified – through invisible and opaque networks – is problematic.

The classification as a threat to the social order depends on the way that deviance (deviant behaviour or appearance) is coded in the technological system. However, selecting which behaviours are indicative of deviance is not at all self-evident. For example, what behaviour signals the presence of a potential thief? In order to identify a thief, police officers and camera operators rely on a set of normatively based, contextual rules that draw their attention to any behaviour that disrupts the 'normal' (Norris, 2003, p. 265). Behaviours are thus suspicious, if they are unusual. For instance, on a busy street people who are running rather than walking, standing still rather than moving, and sitting down rather than standing are unusual and may therefore be considered suspicious. Similarly, those who appear 'out of place' through dress or appearance, those who try to keep away from the camera's gaze and those who mask their face are also deemed suspicious (Norris & Armstrong, 1999). These proxies are also used by engineers coding 'suspicious behaviour' in technological surveillance systems. Digital video cameras of the *SLL*, for instance, have embedded capabilities in order to detect a 'suspicious walking pattern'. What this means in practice, is that the camera detects the types of 'abnormalities' mentioned by Norris and Armstrong (*ibid.*).[167] However, through data mining new proxies might be 'discovered' based on correlations (rather than causal relations). For instance, there might be a correlation between being good at playing darts or wearing a certain brand of sneakers and aggressive behaviour.

166 This is in line with the position that the differing modes of power (as found in the various conceptualisations of surveillance in Chapter 2) do not succeed each other, rather they can and do exist alongside each other; only the dominant operational logic changes with place and context.

167 Precisely how this is coded into the digital cameras is unknown to the author.

However, these types of proxies are just that – proxies. People also run when they are trying to catch a train, those obscuring their face might only be trying to escape the biting effects of the northern wind, and some people simply wait for friends or loiter on the street for lack of anything better to do. Such strategies for detection of deviant behaviour have thus been described as 'largely unproductive in identifying the deviant' (Norris, 2003, p. 265). And proxies identified through data mining might simply be based on spurious correlations (Hildebrandt, 2006a). What these surveillance practices certainly do achieve is that they determine who gets individual and prolonged scrutiny by surveillance technologies; they determine who is slowed down, harassed or excluded. As such, they potentially create inequalities in treatment and experiences of people (Monahan, 2018).

Scenario 3:

Mohammad, Hakim, Harry and Mirko, a group of four young males, two of which have hoodies covering their heads, approach the Stratumseind street. The *SLL* 'smart' video cameras quickly notice them and focus prolonged surveillance on them, as they have been engineered to detect groups of four or more males and those persons wearing hoodies. These categories have been chosen as proxies of deviance based on past experience with troublemakers on the street, which were oftentimes young males moving in groups of four or more and wearing hoodies in order to hide their heads. In practice, these proxies also result in targeting persons of specific ethnic background (e.g. Turkish, Moroccan), as it did in this case. The *CityPulse* system categories this group as 'medium risk' (ie. 'police backup needed') and advises that the police be mobilised on the street in order to question them. The group is stopped, identified and questioned as to their plans for the night. Before they are allowed to go on their way, the police officers notify them that they have been profiled as a risky group and that they will be closely surveilled by the sophisticated surveillance system that is employed on the street within the *SLL*. The group stay on Stratumseind but feel discriminated against and uncomfortable, as they are aware of their close scrutiny.

Scenario 4:

We can also imagine the above scenario with a different ending. During the stop, the police determine that Hakim was involved in a fight in the vicinity of Stratumseind in the past, was arrested but not charged and has been put on an unofficial list of troublemakers held by the city guards and the local police. Because of this they decide to exclude Hakim from the nightlife street. They also exclude his companions that night, even though they were not on the list – they were simply determined deviant by association (and might be put on the list just for this reason). All of them are upset with this decision. Hakim because that fight had happened a while ago and he has not been in any such trouble since; he considers that he will always be a troublemaker for the police. Mohammad, Harry and Mirko were upset because they have not done anything that would deserve exclusion except socialise with their good friend Hakim. They felt that they were treated unfairly, that their identity was determined by other, thus losing another part of any trust they might have had in the local authorities.

So, what are the privacy-related risks stemming from these surveillance practices, in particular, those privacy risks that go beyond the risks of collecting personal data (and which are a primary concern of data protection law)? There are two main types of privacy-related risks that stem from the above scenarios – those that relate to identity development and those that relate to social relations and sociability.

2.3.1 Group profiling – risks for identity-development

In scenarios 3 and 4, where four young males are singled out and excluded, we can see possible detrimental effects for identity-building. As I have discussed in Chapter 3, the development of identity is nowadays considered as intersubjective (Jenkins, 2014; Ricoeur, 1994). In other words, self-consciousness needs to be recognised by another self-consciousness in order to exist. However, the relationship of looking at each other can constitute the site of mutual recognition, misrecognition or denial of recognition of the other (see Honneth, 1995). On the one hand, persons need visual attention to get the social recognition they need (in order to constitute themselves as subjects), on the other hand, its intensity, for instance in staring, can be very intrusive and disturbing. Privacy in some form of control over access to one's self (e.g. one's body, appearance, thoughts, activities) is thus needed in order to regulate this need for more or less visibility. Surveillance alters these processes by undermining their open-endedness (J. E. Cohen, 2017).

While surveillance can have a positive effect of recognition and care (I examine this in Section 2.4), it can also transform persons into objects being watched, especially when dealing with the inhuman gaze of technology, such as video surveillance. Inherent to this unidirectional gaze is a sort of dehumanization of the observed. The sight of the object *as* an object stimulates its use as an object. The person captured by surveillance technology, namely, is passive; only the person conducting the surveillance (the one behind the screen) can be active. Surveillance is thus a technique of power. An example of this can be found in the abuse that occurs behind the screen by the watchers, which are predominantly male, including instances of zooming into and recording of women's private parts for personal pleasure (Koskela, 2002). We can see this effect of surveillance particularly in Scenario 2, where the boys know that they are being watched closely and can do little about it.

Another, perhaps more nefarious, privacy-related risk can be found in the way in which digital networked surveillance often works – through the fragmentation of individuals into dividuals (Deleuze, 1992). What is of relevance, especially for surveillance-based decision-making (including prediction- and pre-emption-based actions), is no longer the physical body of the individual (or the *ipse* identity) but the representation of parts of individuals as inferred from data. Such construction uses statistical commonality to determine class, race or dangerousness in an automatic way, while at the same time defining the actual meaning of these classifications. Moreover, individuals are no longer examined as complete or uniform beings, instead the *self* of the individual is disintegrated and disseminated. This results in the creation of subjects through databases that do not replicate the original subject (they do not even try to) but create a multiplicity of selves that may be acted upon without the knowledge of the original. Notably, these dividuals are increasingly more important for social identity and various types of decision-making than bodily selves (Graham & Murakami Wood, 2003; Lyon, 2001; van der Ploeg, 2003).

In this sense, Cheney-Lippold (2011, p. 165) talks about a 'new algorithmic identity' – identity formation that works through mathematical algorithms to infer categories of identity on otherwise anonymous beings. This is a new type of construction of identity, based on group profiling, where individuals are judged by group characteristics (often based on statistics), which they might or might not possess as individuals (Schermer, 2011). The characteristics of a non-distributive group profile may namely be valid for the group and for individuals as members of the group, but not for individuals as such. Whereas a distributive profile identifies a group of which all members share all the attributes of the group's profile, not all members share all of the group attributes in a non-distributive profile (Hildebrandt, 2008b, p. 21). For instance, when persons

who wear Vans 'Anti-social social club' sneakers are 34% more likely to participate in a fight than other people in the Netherlands, this characteristic holds for the group (i.e. those who wear these sneakers), for the individuals as members of that group (i.e. randomly chosen persons from the Netherlands wearing these sneakers), but not for the individuals *as such* (i.e. for Mirko and Harry who wear them; example adapted from Schermer, 2011, p. 47). Persons in a non-distributive group profile do not necessarily share the relevant attributes. As such, one cannot apply the profile to members of the group without qualification. Moreover, these identifications are largely made *for* and *instead of* us, mainly by corporations who own the algorithms. Individuals are, thus, losing control over the definition and creation of their identities (Cheney-Lippold, 2011, p. 178). Moreover, the identification of particular groups within populations thus largely occur through the marketing logic of consumption, even when not used for marketing purposes, such as, when used for law enforcement and maintenance of public order purposes.

This is particularly important in the case of the *SLL*, which operates in the largest nightlife area in the city and mostly attracts young persons (Kalinauskaitė et al., 2018). Surveillance practices within the *SLL* may thus seriously affect the identity construction of young persons who are still in the midst of the process of developing their identities and which are very malleable.[168] This will be particularly important for the youngsters from Scenario 4. First of all, for Hakim who was clearly classified solely as a troublemaker, following the idea, 'once a troublemaker always a troublemaker'. It did not matter that Hakim had not been in fights since then. And, second of all, for the other three youngsters, who realised that their categorisation depended primarily (or only) on the persons they socialised with, rather than their own actions or their own perceptions of the self. These classifications can greatly affect the way the boys see and build their own identity in the future. The influence of other people's appraisals of ourselves on our conception of the self may be so strong that we end up internalizing them. If others, especially in the case of authorities, perceive us as troublemakers, we are more likely to accept this classification and act in this manner in the future, thus limiting the possibility of change and improvement in life. This has been called the 'labelling bias', which occurs when we are labelled, and others' views and expectations of us are affected by that labelling (Fox & Stinnett, 1996). These expectations can be so powerful that they might turn out to be self-fulfilling prophecies and affect (young)

168 Of course, persons (can) further develop their identities throughout their lifetime, however, the foundational aspects of this construction nevertheless take place during the persons' youth (A. Simmel, 1971; referring to Erikson).

persons' self-esteem (Taylor, Hume, & Welsh, 2010). This becomes a serious danger if we are repeatedly labelled and evaluated by others in a particular way (Jenkins, 2014).

Something similar can be claimed about Scenario 2 as well, although to a lesser extent. This is connected to the way the term 'escalated behaviour' is defined and employed within the *SLL*. The term is defined in such a broad and abstract manner (e.g. crossing boundaries that one would normally not cross; see Chapter 1) that it can include many common and innocuous (although unpleasant) actions, such as the mentioned fight with one's partner. Furthermore, its meaning can also change in relation to the goal and the political climate. When the political climate is tense, as in times of potential terrorist attacks, the term can be understood in a broader and more inclusive manner, restricting more types of behaviour. In this sense, the definition of the category 'escalated' is positioned as a modulating category, where the meaning (and thus the surveillant attention) can be modified continually according to the particular context and even according to each subject's behaviour, but according to logics that are ultimately outside the subject's control. This also means that people can increasingly be categorised as 'deviant' or 'anti-social' and this categorisation is done in an opaque manner, thus removed from most forms of critical participation. Moreover, this categorisation is not concerned with Freek or Marloes individually, rather with a refined type of categorisation into a group profile. This categorisation is potentially affecting people's choices in life, ranging from exclusion from a pub or a street to being put on a law enforcement list of 'deviant' persons (as is claimed to be happening in Utrecht; Naafs, 2018). This leaves little room to get drunk, make mistakes and experiment more generally, which not only takes place at home and in other private places but also in public space (traditionally conceived as the locus of free choice; von Hirsch & Shearing, 2000), particularly nightscapes. Yet, such experimentation is essential, especially for young people.

2.3.2 Exclusion and close scrutiny – risks for associational privacy and sociability

Exclusion has been traditionally used in relation to privately-owned spaces (later also those with public functions, such as shopping malls; Wakefield, 2000) but is now increasingly used in publicly owned spaces as well, both as a crime prevention strategy as well as for exclusion of non-criminal conduct (von Hirsch & Shearing, 2000; see also Chapter 4). This includes (1) profiling – the exclusion of persons who are believed to represent a risk either of nuisance or of criminality; and (2) pre-emptive exclusion of persons who have been found to have committed crimes (or even non-criminal conduct), thus deemed to be 'bad risks' (cf. von Hirsch & Shearing, 2000). Both of these can be seen in Scenario 4. On the one hand, the exclusion of Hakim can be seen as a pre-emptive exclusion because he is perceived as a bad risk for having

committed a prior offence. Such profiling bypasses volition: the person is excluded before he has any chance to show whether he is willing to behave properly. And what counts is not his actual criminal or even 'escalated' behaviour, but his membership in a category of persons considered to represent higher risks (*ibid*.). On the other hand, the exclusion of Mohammad, Mirko and Harry, Hakim's companions, can be seen as a result of profiling, as they are perceived as a risk for future nuisance or criminality based primarily on their association with Hakim.

While exclusion might not be a privacy concern as such, it entails a loss of freedom of access and of movement. As I will show, this measure indirectly affects privacy, especially associational privacy, related to the development and maintenance of varied and meaningful interpersonal relationships (Fried, 1984; Rachels, 1984; Roessler & Mokrosinska, 2013; these freedoms are also connected to Article 8 ECHR, as I discuss in Chapter 6).

Freedom of access and of movement relate particularly to public space, which is traditionally conceived as a space of freedom, in which persons are entitled to move about at will, as long as their behaviour does not violate relevant regulations (see Chapter 4). Freedom of movement means that a person should be able freely to come and go, without the need to justify her presence. However, these freedoms also assure everyone access to common facilities and the social goods that public spaces provide (von Hirsch & Shearing, 2000).[169] A person excluded from a part of public space is potentially not only barred from access to important goods and service (for instance, when she is barred from an area where the only close-by stores are located),[170] she may also be excluded from recreational facilities and the variegated aspects of social life that take place in such locations. As such, limiting the freedom of access and movement can lead to the limiting of opportunities for social interaction (that is development and maintenance of social relations) and the forming of one's social identity – another key value closely connected to privacy.

169 Furthermore, public space also performs a 'corridor' function – it permits movement from one private space to another. If one is barred from public thoroughfares, she cannot visit her friends in other places, even if they invite her.

170 As was the case in CIN Properties Ltd. V Rawlins [1995] 2 EGLR 130, where a person was barred from a local shopping mall in Wellingborough, serving as the city's principal shopping and congregating space. Persons excluded from the mall were unemployed youths who had not been found guilty of any offence but were deemed nuisances by the mall owner. However, exclusion meant that the youths were also barred from the locality's primary shopping and recreational area. For a discussion of the case see Gray and Gray (1994).

In the case of the Stratumseind nightlife street, exclusion from this area means exclusion from an important part of social life, especially for young persons. The interests of privacy as a means to enable social relations is particularly important in semi-public and public space, as relationships often take place outside strictly private places or intimate settings (Koops et al., 2017). This is an increasingly important aspect of privacy, which has also been recognised by the European Court of Human Rights (discussed in the following Chapter).

'Mere' close scrutiny in public space, rather than exclusion, also affects associational privacy. Privacy research has shown that social relationships can become defective in some way when privacy of the relationship is invaded through external surveillance (Roessler & Mokrosinska, 2013). This can be seen from Scenario 4, in which Harry, Mirko and Mohammad were excluded (and first closely surveilled) from Stratumseind because of their association with Hakim. A similar situation would occur, if only Hakim would be excluded, whereas the other boys would be allowed to stay (and to return in the future) on the condition that they would no longer socialise with Hakim. Surveillance on the street (and possibly elsewhere) could control whether they would abide to this rule. Harry, Mirko and Mohammad would thus be confronted with a tough choice – either to continue socialising with Hakim and be excluded (and put under targeted surveillance) or to stop socialising with him and join in on the fun on the Stratumseind street. In this sense, targeted surveillance of public sense could potentially lead to defective relationships.

However, such surveillance does not only pose risks for individual relationships, it also poses risks for society and social life more broadly. Surveillance can namely affect the sociability and openness of public space, particularly by affecting the level of trust. Democracy requires both inclusion and connection among citizens. This is important for two general reasons: first, because community is only possible if interpersonal communication and social encounters exist; and, second, because individuals, groups and crowds need a common 'stage' where – visible to others – they become political subjects. Citizens thus need to be able to communicate with each other in a common (public) space, which extends beyond the primary (intimate and other close) associations. While the expansion of surveillance might make some people feel safer (although that has also been disputed; see e.g. Norris, 2003), it also leads to increasing fear, distrust and even racist paranoia among people (Davis, 2006; Ellin, 1997). If too many places are under (potentially) indiscriminate surveillance, then everyone that is present there might come to feel untrustworthy. Moreover, assuming that there is a reason to put a high level of surveillance in a particular public space, one might begin to look at others – strangers – in public space with an increased level of suspicion. We

can go even further and say that in order to protected oneself from the risks and from being cast in the category of risk, we develop vested interests in a dense network of surveilling, selecting, separating and excluding measures: 'We all need to mark the enemies of security in order to *avoid being counted among them* … We need to accuse in order to be absolved; to exclude in order to avoid exclusion' (Bauman & Lyon, 2013, p. 104; emphasis in original). This can negatively affect persons' capacity to tolerate difference and dissent, which is a necessary and desirable part of life in public space (see Chapter 4).[171]

It would be a bit of a stretch to apply this argumentation directly to the *SLL* example. The Stratumseind street is only one street and a nightlife street at that, relatively empty during the day. Even if access and behaviour there would be controlled to a high extent that would not likely affect the general level of sociability in the public space of Eindhoven. It might simply lead to a decrease in visitors of the street, which would no longer seem fun or exciting (as a nightlife street should). However, as I have already speculated in regard to the *Trillion* app, the app and surveillance on the street more broadly might be used in such a manner so as to target ethnic minorities or other groups that are already stigmatised. Moreover, a decrease in the level of sociability of public space might occur if the surveillant logic such as the one within the *SLL*, should spread to other parts of the city, as might happen with the promised transformation of Eindhoven into a smart city.

2.4 Goals of the surveillance: influencing behaviour in the name of safety and profit and risks for autonomy

The overarching goal of the sensor-based surveillance within the SLL is to monitor and influence the behaviour of persons on the street in order to create or preserve a positive atmosphere on the street and a safe environment, which would in turn draw more people to the pubs on the street (Kanters, 2013). This main aim thus combines, in a very intertwined manner, both public (safety) and private goals (profit). The aim is also very much future oriented. For instance, fights and other types of escalated behaviour are sought to be prevented or even pre-empted (although these goals were not achieved in practice during the operation of the *SLL*; see Chapter 1). This is to be done via digital technologies on the street, capturing a specific dimension of activity or behaviour across the monitored space, such as walking patterns or crowding levels

171 As judge McQuillan put in People v. Collier (1975): 'Unwarranted police surveillance will destroy our capacity to tolerate – and even encourage – dissent and non-conformity; it promotes a climate of fear; it intimidates, demoralizes and frightens the community into silence.' Available at: https://www.leagle.com/decision/197561485misc2d5291490 (accessed 31 March 2019).

(additional dimensions such as mood, gait or even drinking patterns could potentially also be captured).

Scenario 5:

The common scenario that the *SLL* imagines goes like this. If video cameras detect crowding on the street, sound sensors detect higher levels of noise and several negative tweets are captured by the social media analysis (see Image 11 below), the atmosphere on the street might be classified as 'tense', that is, potentially leading to aggressive behaviour. The situation on the street might thus be categorised as 'medium risk' by the *SLL* surveillance system and police presence might be considered unnecessary at this point. Instead, the special lighting system with a soothing lighting scenario using warm colours would be automatically turned on and the smell of oranges would be dispersed in the street. The tense atmosphere would be 'de-escalated' and a potential fight might have been prevented from occurring in the first place. Everyone is now able to enjoy a fun night out in their favourite pub.

One aspect of the surveillance taking place within the *SLL* is oriented towards the enhancement of safety on the street, which has had (and seems to still be having) issues with violence (Schuilenburg & Peeters, 2018).[172] There is thus an element of care present in these surveillance practices. Despite the widely accepted claim that surveillance is an ambiguous practice, showing elements of both control *and* care (Lyon, 2001), the positive aspect of surveillance is often omitted in surveillance scholarship. The 'smart design' found in the *SLL* example (in particular in the *De-escalate* project), however, also has positive attributes, which Schuilenburg and Peeters (2018) have theorised through Foucault's concept of pastoral power. According to Foucault (2007, p. 127), pastoral power is a 'power of care' that aims for the wellbeing of the 'flock' (the population) by constantly observing and managing daily life. The shepherd not only watches over the herd as a whole, but also looks after every individual sheep, ensures that the sheep do not suffer, goes looking for animals that have gotten lost, and treats animals that have been injured. This can be seen as a part of 'positive security', an emerging concept representing a means to improved urban safety and security by strategies based on positive attributes of living together, such

172 See also news reports of violence on the street: van Arensbergen, W. (2018, January). Waarom heeft politie verdachte van mishandeling op Stratumseind nog niet, met al die camera's? ED. Retrieved from https://www.ed.nl/eindhoven/waarom-heeft-politie-verdachte-van-mishandeling-op-stratumseind-nog-niet-met-al-die-camera-s~a7dda208/.

as care, protection and belonging (Schuilenburg & Peeters, 2018, p. 2). This strand in scholarship suggests that the architecture of security as found in smart cities (at least in the West) 'focuses less on surveillance and exclusion and more on "scripting" the use of public space by designing in new defaults for behaviour' (*ibid*.). As such, it is said to be protective, inclusive, preventative and caring; it does not simply exclude or defend against unwanted behaviour.

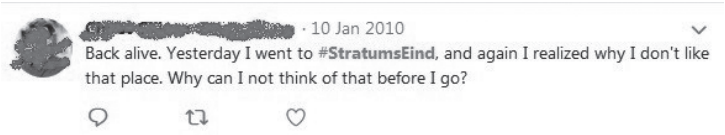


Figure 5.4: *An example of a negative tweet about the Stratumseind street*

In the case of the *De-escalate* project, 'psychological triggers are used to stimulate an efficient, safe and consumption-focused use of space through architectural interventions that intend to mould the behaviour of the user of that space' (*ibid*., p. 5). Schuilenburg & Peeters (2018, p. 6) thus argue that the *De-escalate* project is 'profoundly pastoral in nature'. While I agree that a fair level of general concern and good intentions are indeed present within the project, I posit that their claim is too far-reaching. Pastoral power is imbued with the concern for the needs not only of the 'flock' in general but also of every separate member. As such, it depends on a detailed knowledge of each member of the flock.[173] This individual knowledge or concern does not seem to be present within the *SLL* projects. The *De-escalate* system (or its managers), representing the modern day 'shepherd', has no individual knowledge of Freek and Marloes, and as long as they respond as planned to the soft 'nudges' of the lighting scenarios and orange smell, they are no longer of interest. It has even less concern for Hakim, Mohammad, Harry or Mirko, in regard to whom the only thing that matters is that they have been profiled as a risky group, which needs to be excluded at the first sign of deviant behaviour. Or that Hakim is a 'known troublemaker', so that he and his companions need to be excluded from the Stratumseind street even in the absence of deviant behaviour. In these latter two examples, the logic of surveillance is exclusionary – the logic of control – rather than the inclusionary logic of care. Here we see well how surveillance can represent different modes of power and serve various strategic objectives, which also support and augment each other: on the one hand,

173 'The pastor must really take charge of and observe daily life in order to form a never-ending knowledge of the behaviour and conduct of the members of the flock he supervises' (Foucault, 2007, p. 181).

exclusion (or 'fencing out') and, on the other, confinement (or 'fencing in') (Bauman & Lyon, 2013, p. 64).

Moreover, the general goal of the project (including that of the *SLL* and the *Stratumseind 2.0* umbrella project more broadly) could be described as pastoral only with difficulty. As Schuilenburg & Peeters (2018) note themselves, the goal of the *SLL* is 'consumption-focused use of space'. The Stratumseind street is, of course, a nightlife street composed mostly of night-time pubs. The consumption referred to then is consumption of drinks, especially alcoholic beverages, including beer (remember that some of the parties of the Stratumseind 2.0 are large Dutch or multinational breweries). Surveillance on the Stratumseind street is thus again in line with Foucault's concept of security, which wants to optimise consumption, while at the same time minimising labour and other expenditures through the risk management of multiplicities (Harcourt, 2014, p. 12). The operational logic of security can be described as inclusionary, as it is aimed at managing – that is influencing behaviour – of persons in order to preserve the flow, particularly persons' consumption (think of Freek and Marloes in Scenario 2). This means that persons are managed *en masse* (as flows) in a way that maximises consumption, while at the same time minimising labour and other expenditures. In this sense, public space can be said to be transformed into quasi-public space or, as Harcourt (*ibid*.) calls it, 'themed space' (see Chapter 4).

However, this management is highly dependent on the capture and analysis of a large amount of data about us (although not necessarily directly identifiable data). As such, in themed spaces we are invited (or even nudged) into exposing ourselves, that is, tweeting, posting pictures on social media, dressing in a certain way so as to attract the camera's view. While visitors of the Stratumseind street are not yet nudged into exposing themselves (although persons are invited to expose others within the *Trillion* project), this might well be the direction in which it would develop in the future. Nevertheless, the behaviour of visitors of Stratumseind is attempted to be influenced through the use of light and smell. According to Schuilenburg & Peeters (2018, p. 6), the *De-escalate* project seeks to provide incentives or 'scripts' for desirable behaviour. 'A "script" is not just [a] set of directions, it is rather the "designing-in" of "prescriptions" that impose themselves on the visitors in the most direct sense: through light, smell and sound, people's mood and – by extension – behaviour is influenced' (*ibid*., pp. 6-7). This can be seen as a shift from discipline (self-monitoring for the purpose of improvement) to control, which is enacted through practices external to the body. This shift has been described as an example of corporate logic (Cheney-Lippold, 2011, p. 169; Deleuze, 1992), which is not interested in long-term goals and the improvement of persons (or society more broadly), as long as their short-term goals can be reached

by influencing external behaviour. This corporate logic now seems to have been transplanted into municipal governance, at least to a certain extent.

As mentioned above, there is an intertwined double goal at play within the *SLL* – people's behaviour is (attempted to be) influenced both for the sake of safety as well as for profit. It does not come as a complete surprise then that on the Stratumseind street potentially conflicting types of nudging are found. On the one hand, visitors of the street are nudged (by presenting the street area as an attractive nightlife destination) into visiting the pubs, staying there longer and, consequently, drinking more. On the other hand, *SLL* sensors closely surveil the visitors in order to detect escalated behaviour, which they could then de-escalate or, if unsuccessful, exclude the persons from the pub and/or the street. The two goals are, of course, not necessarily conflicting. One might argue (in a less nefarious way) that the surveillance practices within the *SLL* are aimed at optimising the Stratumseind experience – that is, to induce people to drink precisely the right amount of alcohol that makes them feel great without getting drunk. The two goals together could thus be seen as nudging the non-drinkers into drinking more and the heavy-drinkers into drinking less. Nevertheless, such individualised influence is highly unlikely given the current capabilities of the technologies within the *SLL* (I discuss this further below).

Scenario 6:

The atmosphere on the Stratumseind street is 'sleepy' and 'boring'. Persons are drinking their beers slowly and a high number of people is captured by the *SLL* system as leaving the street (potentially to go to the Dommelstraat, a rivaling nightlife street in the centre of Eindhoven). The lighting system is turned on, deploying a scenario with brighter lights in order to make the atmosphere livelier and make people feel like they want to stay longer in the pubs and spend more money there, preferably drinking beer. Once the visitors of the street have done precisely that – that is, got tipsy or drunk – the *SLL* sensors watch them closely in order to detect any escalated behaviour that they could then de-escalate or, if unsuccessful, exclude the persons from the pub and/or the street.

Scenario 7:

After a winning match against PEC Zwolle, PSV fans (the main Eindhoven football club) go to celebrate on the Stratumseind street. They have something special planned for this night – a small protest against the increased surveillance of football matches at the PSV stadium and the surveillance taking place on the Stratumseind street, their usual place of celebration. At the stadium, during the break of the match, fans already put up large signs of protest, on which it is written: 'We are not criminals. We are not movie stars. We are football fans.' They want to do something similar on the Stratumseind street with the intention that their protest be captured on the various types of surveillance technologies on the street, thus potentially receiving more attention both from the municipality and the media. When the fans approach the street, already chanting in protest of the surveillance, they are noticed by Merel, the concerned citizen with the Trillion app on her phone. She immediately reports the 'shouting and gesturing of a large rowdy group of football fans, probably going to the Stratumseind street'. The *SLL* surveillance system soon also detects a rowdy group of visitors (classifying it a 'medium risk situation') and turns on a calming lighting scenario as well as dispersing the smell of oranges. When this does not calm the fans down (quite the opposite, it seems to make them protest even louder, as the fans know that this is the SLL surveillance system in operation), the technological system determines a heightened level of risk on the street and turns on an additional, newly acquired technology, the 'Mosquito'. This technology emits a high-frequency irritating sound, which affects mostly those under the age of twenty-five. Since many protesters are under that age, they are negatively affected by the sound and after several minutes of painful buzzing in their ears they decide to leave the street and rid themselves of the noise. Soon enough, the remaining protesters give up and decide to have a drink in their favourite pub on the Stratumseind street to celebrate the win.

The privacy-related risks concerning these scenarios primarily concern the issue of how the surveillance practices affect our autonomy through influencing our behaviour – both personal and political autonomy as well as the development of multiple and diverse publics.

Figure 5.5: *PSV football club fans protesting against increased surveillance of matches on 19 December 2015 (copyright Samantha A. Adams)*

2.4.1 Manipulative nudging – risks for personal autonomy

As I have discussed in Chapter 3, autonomy is commonly considered as a key argument for why we value privacy. There are possible risks for autonomy stemming from the fact that contemporary cities or parts of them are being increasingly transformed into an extraordinary apparatus of data capture (of persons' interests, preferences, desires, emotional states, beliefs, habits and so on), which was previously only possible within research laboratories and high-surveillance institutions like prisons or mental institutions. Cities can thus be said to be developing into large laboratories, where a key question posed is: how to render the behaviour of persons predictable and externally controllable? In this sense, the *SLL* can be described as *manipulating* the environment in order to discover and influence how people behave so as to make the place safer and more attractive for visitors. This type of development has often been called nudging (e.g. Schuilenburg & Peeters, 2015; van Dijck & Poell, 2015).

A nudge is commonly defined as 'any aspect of the choice architecture [that is, the context in which people make decisions] that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives' (Thaler & Sunstein, 2009, p. 6). The concept of nudging is based on the fact that much individual decision-making occurs subconsciously, passively and unreflectively rather than through active, conscious deliberation. The environment (the 'decisional choice context') can thus be intentionally designed in ways that systematically influence human decision-making in particular directions. Nudges have

been commonly criticised in literature for having manipulative effects that bypass autonomous decision-making, thus positing a risk for our autonomy (e.g. Yeung, 2017). However, before such a claim is made, a brief discussion of the distinction between nudging, manipulation, persuasion and coercion is needed.

According to Susser, Roessler and Nissenbaum (2019) there are some subtle but important differences between these types of influence. They posit that manipulation, at its core, is hidden influence – the covert subversion of another person's decision-making power through exploitation of the person's cognitive (or affective) weaknesses and vulnerabilities (*ibid*., p. 2). This is in contrast to rational persuasion, which can be defined as the forthright appeal to another person's decision-making power (that is, giving reasons a person can reflect on and evaluate, where the decision is ultimately left to the person), or coercion, which is the restriction of acceptable options from which a person can choose (that is, making 'irresistible incentives') (Rudinow, 1978; Susser et al., 2019, p. 2).[174] Both persuasion and coercion attempt influence in a forthright manner without undermining a person's decision-making powers. Manipulation, by contrast, is to deprive the person of 'part authorship' (Raz, 1986) over their actions.[175] Part ownership, rather than full ownership, because individuals are social beings who exist inexorably among others and these others affect us. Thus, according to Raz (1986, p. 20; as cited in Susser et al., 2019, p. 13) 'an autonomous person is part author of his own life. His life is, in part, of his own making.'

174 Susser, Roessler & Nissenbaum (2019) give an example of a car-dealer owner who wants to make her employees work longer hours. 'To persuade her sales team to work longer hours she might argue that people shopping stay out later during long summer days, so (given that it's summer) working late would increase their odds of winning extra commissions. In this way, she appeals to her team members' own ends—earning an income—and tries to show them that behaving the way she wants is a means to achieving them. She attempts to influence her team by changing the way they understand their options (i.e., by appealing to their internal decision-making process). If her argument fails the manager can shift strategies: instead of offering an argument she might offer an incentive, such as overtime pay. Rather than change how her team members understand their situation, the manager changes the situation itself' (Susser et al., 2019, p. 11).

175 However, manipulation does not mean simply to make less than ideal decisions than one otherwise would. For example, someone trying to quit drinking alcohol receives a coupon from Altstadt, a café on the Stratumseind street, for free drinks for you and 3 of your friends. This coupon cleverly tempts you – not only to drink beer (your favourite beverage of choice) but also to be able to treat your friends with it and have a fun night out with them. Surely, you are tempted but you have not been given an irresistible incentive – you have not been coerced. But this is also not manipulation – '[i]f you can resist it, and yet you don't, then you have simply been persuaded by bad reasons' (Susser et al., 2019, p. 15), rather than being deprived of (part) authorship.

Based on this brief description, we can determine how nudging relates to manipulation. First, we need to observe that there are many different types of nudges. Some are forthright and aim to appeal to people's deliberative capacities. For example, simple disclosures (a type of 'informational nudge'), such as nutritional labels on food, try to trigger persons' deliberative capacities. However, there are other types of nudges, which can be manipulative, if they are hidden and exploit cognitive weaknesses or vulnerabilities. Furthermore, manipulation is usually targeted – in order to exploit one's vulnerabilities, one must know what they are and how to leverage them (Susser et al., 2019, p. 21). Most nudges, however, are not targeted to particular individuals, they are applied to everyone in the same way. A speed bump on the road affects all who pass it. However, ICTs are well-suited to facilitate nudging that would allow for 'fine-grained microtargeting', turning manipulative nudging into what Yeung (2017) calls 'hypernudging'. Hypernudges are not only hidden but they target and exploit individual vulnerabilities, making them very difficult to resist.

Two types of activities within the *SLL* can be classified as nudging – the use of lighting scenarios and of smell with the aim of influencing people's behaviour ('de-escalating' aggressive behaviour and, potentially, 'escalating' it). Within the *SLL* they employ the generic term 'influence' (*invloed* in Dutch), a term without normative baggage. But could these practices be called manipulative? First, they are hidden. While we can detect special lighting (e.g. a reddish or blueish colour instead of the usual 'white' or 'yellow') and smell (the smell of oranges) on the street, we do not necessarily notice them, especially when we are focusing our attention to something else and are potentially intoxicated. Moreover, we would also likely not know the purpose behind the special light or smell and how they function. Second, these nudges do not appeal to people's deliberative capacities; instead, they exploit our cognitive weaknesses, albeit for a generally positive purpose – 'de-escalating' aggressive behaviour. If we are getting angry, for example, colder light (in the shades of blue and green) and the pleasant smell of oranges, supposedly make us feel calmer (de Kort, 2015). And, finally, these nudges try to influence people as a group – all of the visitors of the Stratumseind street, thus are not able to precisely target and exploit individual vulnerabilities.

As such, it seems fitting to describe the nudging taking place within *SLL* as a (relatively) easily resistible manipulative practice for a benevolent purpose (when used for de-escalation of aggression, at least).[176] This is in line with the lack of success

176 Here I speak of a 'manipulative practice' because manipulation is a 'success concept' – it presupposes the effect of manipulation (Wood, 2014). In the case of the *SLL*, this success has not been shown, so it is more appropriate to speak of manipulative practices.

of the *De-escalate* project, which did not lead to any demonstrable effect on persons' escalated behaviour. For the same reasons, I would posit that there is little risk of successful manipulation in the case of nudging for the purpose of 'escalation' (making the mood on the street livelier for purposes of increased consumption) in Scenario 5.[177] Would the nudging practices on the Stratumseind street become capable of individual exploitation of vulnerabilities and weaknesses through more sophisticated digital technology, however, the risks for manipulation – and thus for autonomy – would become much higher. Such a development might not take place within the *SLL*, but it is not unimaginable that further development in digital technology would not make it a real possibility. Given the enthusiasm of adopting technological 'solutions' in cities and a lack of legal restraint (apart from data protection law), technologies capable of targeted effect on our decision-making processes might be found in future (smart or dumb) cities.

2.4.2 Chilling effect and coercion – risks for political autonomy and the development of publics

As I have discussed in Chapter 3, privacy is also important because of its value for democracy, particularly in relation to political autonomy and the development of multiple publics (Brettschneider, 2007; Regan, 2015). Indeed, most conceptions of democracy 'rest on some sense that people are able to think and make judgments for themselves' (Bauman et al., 2014, p. 137).

However, citizens who are subject to pervasive, networked surveillance and modulation for commercial and/or political interests are said to increasingly lack the capacity to practice active, critical citizenship (J. E. Cohen, 2017). This is connected to the fact that such techniques of power are either *functionally* invisible because people no longer notice their relationships and interactions with the technologies or they are *physically* invisible, because they are intangible, hidden or embedded in the existing infrastructure of public space (Sadowski & Pasquale, 2015). They can thus seriously hinder an individual's (personal and political) autonomy as they target one's cognitive weaknesses, rather than promoting habits of mind, of discourse and self-restraint that are required for informed and reflective citizenship.[178] In a similar manner, Brownsword

177 There are, of course, differences between people – some are influenced more easily than others.

178 This is further connected to issues of information access and social interaction with an instrumental, market-oriented instrumentality (mostly through platform-based information businesses), where we find the (potentially) continuous adjustment of the information environment to each individual's perceived or inferred comfort level (J. E. Cohen, 2017). In this sense, Cohen speaks of a 'modulated citizenry'.

(2006) argues that people will lose the ability to make moral choices when regulation becomes embedded in design and – after some time – is no longer noticed as being regulatory. This type of power therefore does not immediately affect what persons can do (their potentiality) but rather their 'impotentiality' – what they cannot do (Agamben, 2011).

In Scenarios 6 and 7, I have imagined a possible use of surveillance technology, which directs persons' behaviour towards commerce ('uninterrupted consumption') and away from other activities, including protest. In Scenario 7, after the use of 'soft' nudging through light and smell failed to calm down the 'football-fans-turned-protesters', another 'harder' type of technology for influencing behaviour was used – the 'Mosquito'. This technology then led to the dispersal of young protesters, putting a quick and simple end to the protest. Based on the discussion in the previous section, we can determine that this technology functions through coercion rather than manipulation or nudging. The high-pitched and irritating noise namely restricts the acceptable options a person can choose – after a short while a person has no other acceptable option but to leave the place in which the buzzing is heard. While done in a relatively subtle manner of intervening through technology (at least in comparison to violent suppression of protest), the municipality (in cooperation with private actors) essentially coercively put an end to a protest.[179]

What can also be seen from Scenario 7 is the potential slippery slope of using ever more coercive ('harder') technologies, when the softer ones fail. In fact, the failing of softer technologies can itself be used as an argument for the implementation of harder technologies.[180] If nudging with light and smell do not seem particularly problematic, at least at first sight, coercion through the 'mosquito' (or similar) technology might. This type of technological intervention in formal civic participation is becoming an increasing reality in various democratic regimes, rather than only being used in

179 I leave aside the question, whether the protesters have duly notified authorities of their peaceful protests and acquired a 'permit' to conduct it. Not doing so would in itself still not be a reason for the use of coercive tactics to prevent the protest according to ECtHR case law (see e.g. Schabas, 2017 on the freedom of assembly and association). Whether the use of the 'mosquito' would be interpreted as a coercive tactic, however, remains unclear.

180 Echoing the classical argument for an ever-increasing need of security measures: the failure of existing security measures is not an argument against such measures, rather it is an argument for more (and more coercive) security measures.

non-democratic ones (Sadowski & Pasquale, 2015).[181] Even in democratic regimes we can observe a shift towards a rapid (ideally pre-emptive) pacification of risks, where technological means are used in order to 'dissuade' crowds from forming in the first place.

Proliferating surveillance in contemporary (smart) cities is tightening the social control by making disobedience and dissent increasingly difficult. On the one hand, this is done through the chilling effect of surveillance (the use of drones with facial recognition during protests and other public activities, such as public celebrations), which might chill spirited expression or the exercise of human rights and freedom, such as freedom of assembly and association. Not only might Mirko, Mohammad and Harry decide to not associate with Hakim (given the potential punishment), others might decide to not associate with any of them, if they were to be regarded with suspicion by the surveillance system (for instance, if they were subsequently stopped and questioned by city guards or the police). Furthermore, developers of smart cities might be tempted to embed 'algorithmic deterrence' into transport and policing systems. In San Francisco, for example, authorities manipulated both train schedules (having trains skip stations at which larger numbers of protesters were expected to board with the purpose of going to the protest) and wifi access in order to disrupt the activity of protesters (Sadowski & Pasquale, 2015).

Furthermore, the tightening of social control, where de-escalation and exclusion are the norm, can also be said to be antithetical to the practice of critical citizenship. 'Liberal citizenship requires a certain amount of *dis*comfort – enough to motivate citizens to pursue improvements in the realization of political and social ideals. The modulated citizenry lacks the wherewithal and perhaps even the desire to practice that sort of citizenship' (J. E. Cohen, 2017, p. 463; emphasis in original). In a tightly scripted public space, where difference is either deterred or excluded, there is no room for discomfort as well as the development of multiple publics with different views, supporting an agonistic type of democracy. Pervasive networked surveillance that profiles and sorts persons is, namely, aimed at eliminating diversity and serendipity required to build robust communal ties, furthermore creating and entrenching

181 In 2014 in Kiev, Ukraine, for example, protesters received an ominous message on their mobile phones from state authorities, which read: 'Dear subscriber, you are registered as a participant in a mass riot' (Sadowski & Pasquale, 2015). Such participation, according to recent laws in Ukraine against public gatherings, can be punished with a sentence of 15 years in prison (Walker & Grytsenko 2014).

distinctions and hierarchies among the surveilled persons (oftentimes connected to socioeconomic status and race) (*ibid*.).

This effect of networked surveillance relevant for society and democracy more broadly, cannot be claimed based solely on the *SLL* example. However, would the surveillant logics of the *SLL* example expand throughout the city of Eindhoven – not completely unlikely given the promises of smart city transformation – these broader risks for democracy would come into play. As such, it is important to be aware of these risks in advance, when they still stem from hypothetical scenarios, rather than becoming aware of them only when the 'train' is going forward at full speed (and turning on the breaks is much harder).

2.5 Perception of the surveillance on the Stratumseind street

It is not possible to properly discuss the perception of the surveillance on the Stratumseind street, as no quantitative or qualitative study of visitors' perception has been conducted. However, based on the analysis of scholarly and journalistic writing about the *SLL*, one can state that the surveillance is not perceived in a completely negative way. Although most journalistic pieces covering the *SLL* are wary of the surveillance and usually refer to it through the use of the Big brother metaphor (e.g. de Graaf, 2015; Naafs, 2018; van Doorn, 2018), some news reports have emphasised the positive – caring – side of surveillance on the street (e.g. Kist & van Noort, 2015). This is so because the street indeed has issues with criminality taking place there, so that action to counter it from the municipality and the police is welcomed. This is also seen is some scholarly writing (e.g. Schuilenburg & Peeters, 2018), in which authors analyse the *De-escalate* project (but not other projects within the *SLL*) through the 'caring' framework of pastoral power.

In this sense, there is room for further research, which would closely examine the perception of the *SLL* and its surveillance practices by the inhabitants of Eindhoven and, particularly, the visitors of the Stratumseind street.

3. CONCLUSION

In this Chapter I have brought together literatures on surveillance theory and privacy theory by examining the surveillant practices within the *Stratumseind Living Lab*. This enabled me to determine not only the particular types and characteristics of surveillance within the *SLL* but also the particular risks relating to privacy stemming from them. Moreover, I have tried to render these as concrete as possible through

discussion of seven short hypothetical scenarios – privacy is, after all, a very much abstract matter.

Within the *SLL*, I have detected several surveillant modes of power. What is clear from the above discussion, is that the principles of panoptic surveillance are largely absent. The emphasis is not on discipline – the surveilled visitors, who are either nudged or controlled into one or other behaviour, are not supposed to internalise the gaze of the *SLL*. In other words, the *SLL* is not trying to educate or improve them from the *inside*. On the contrary, the *SLL* is mainly interested in affecting the visitors from the *outside*. It tries to influence (and sometimes manipulate) their behaviour in order to maintain an uninterrupted consumption flow or to exclude them from the environment entirely. The most prevalent surveillant techniques on the Stratumseind street are thus those from the second stage of surveillance theory. The primary logic is found in Foucault's conceptualisation of security, where the focus is on the 'atmosphere' on the street and persons are governed as a multiplicity, rather than as individuals. As such, the principle of such surveillance is inclusionary – smaller transgressions are overlooked as long as the atmosphere on the street (relating to relationships on the street as a whole) is not affected. In other words, as long as Freek and Marloes kiss and make up and the consumption on the street is undisturbed, law enforcement will not be called for.

Alongside this type of surveillance, the exclusionary logic of control (as conceptualised by Deleuze) might also be operating. This logic would kick in not only when 'security' would fail, it would also be the primary logic to be applied to the undesirables (e.g. thieves, homeless, troublemakers) on the street. Their presence on the street is, namely, not intended to be 'managed', they are to be identified and excluded. In regard to the *SLL*, one can hypothesise that at the first detection of aggression (e.g. raised voice or broken glass) by someone considered a troublemaker through data mining within the *CityPulse* system, the troublemaker will more likely simply be excluded (by city guards or the police) rather than tried to first be calmed down via lighting scenarios. While this scenario remains a hypothesis, it is in line with the general goal of the *CityPulse* system (detection and *prevention* of deviant behaviour), as well as with the general trend in risk-oriented law enforcement and predictive policing practices, including in the Netherlands. Furthermore, surveillance within the *SLL* can also be described as a surveillant assemblage (following Haggerty and Ericson). Consisting of more or less open-ended projects, various types of technologies, actors, subjects (organised in a PPP), relations and goals of surveillance with a seemingly rhizomatic structure, it lacks discernible boundaries. As such, surveillance within the *SLL* can be described as emergent, unstable and lacking clearly accountable actors, so that it cannot be criticised

by focusing on a single institution. While the third stage of surveillance theory, especially participatory surveillance through social media and community policing, is also present in the *SLL*, this type of surveillance is still very limited.

This broad overview of surveillance types and characteristics enabled me to identify the particular risks related to privacy stemming from these surveillance practices. I use the term privacy-related risks, which does not strictly distinguish between privacy and non-privacy risks. Following Cohen (2017), I have employed a broad conceptualisation of privacy, seeing it as enabling *breathing space* to individuals in order to define and redefine themselves as subjects. This definition seems oddly suitable for the type of surveillance, where the focus is on *atmo*sphere. Moreover, privacy is seen as an infrastructural value and right, without which several other values and rights cannot be enjoyed either.

The analysis in this Chapter has revealed several types of privacy-related risks stemming from the *SLL*, including: (re)stigmatisation, diminishing trust, profiling and the production of risk categories, disintegration and datafication of the self, exclusion, hindering social relations, risks for sociability, and narrowing down possibilities for autonomous (both personal and political) action as well as for the development and existence of multiple publics. While these risks are diverse, they can be structured in a few broad types of privacy-related risks. One of these types is the risk of hindering the separation of different spheres of one's life, leading to potential unwelcome consequences in other spheres of a person's life (if, for example, the lists of troublemakers is shared with the boys' school or social services, potentially leading to an increased perception of them as troublemakers or other negative effects). However, the most predominant privacy-related risks stemming from the surveillance within the *SLL* and similar initiatives are those that hinder:

(1) the development of identity (individual, social and political);
(2) the possibility of autonomous action (personal and political); and
(3) social interactions, both in relation to informal daily life as well as political activity occurring in public space.

There are several takeaways from this analysis. A general takeaway is that the risks concern both traditional privacy risks (that is, in relation to the individual), as well as risks relating to society and democracy more broadly, which have more recently been connected to privacy, as well as risks closely connected to the values of public space itself (especially seen in the third type).

More specifically, the analysis has confirmed that a relatively new type of privacy risk is at the fore today – privacy risks concerning groups (most often, algorithmic groups based on profiling). The *SLL* can be said to govern through atmosphere. In line with Foucault's theorisation of the functioning of security, the focus of surveillant activity is on relationships between persons and the environment they are in, in order to affect the general atmosphere on the street, transforming it into an 'atmosphere conducive to consumption'. As such, individuals need not be individually identified, yet they may still be individually 'reachable', that is, subject to consequential inferences, predictions and nudges taken on that basis (Barocas & Nissenbaum, 2014). This issue has recently been recognised in privacy literature under the heading of 'group privacy'. Several scholars have attempted re-conceptualisations of privacy as a type of group privacy, trying to find a way 'to move from "their" to "its" privacy with regard to the group' (Mittelstadt, 2017; Taylor, Floridi, & van der Sloot, 2017b, p. 2; see also other contributions in the edited volume). These first accounts of new conceptualisations, however, have yet to receive sufficient attention and discussion.

Another insight is that in the specific context of smart city and living labs surveillance in public space, the social and political value of privacy are at the forefront. I do not mean to say that the classical individual values are no longer implicated – they still are. However, the two more recent accounts of the broader value of privacy seem to be at particular risk through the new types of surveillant technologies and their manners of operation. Privacy in public space, namely, does not focus on disengaging the individual from social and political life, as follows from the traditional liberal perspective on privacy. Quite the opposite, privacy in public space focuses on facilitating the development of a broad range of social relations, including the aims of political association. Privacy thus has a strong facilitative role here (exhibiting its infrastructural nature), as privacy in public space allows for a more secure and fuller exercise of other rights and freedoms, in particular freedoms of assembly and association, of expression, and of movement.

This is connected to the insight based on Chapter 4, according to which surveillance within smart city/living lab initiatives also shapes the texture of public places in functionally specific ways that may be detrimental to both political and informal community life. It does this particularly by valancing multiple-purpose public spaces for particular patterns of use (Patton, 2000, p. 186). Surveillance of public space within the *SLL* creates an environment that is conducive to consumption (in this case, consumption in the pubs on the Stratumseind street). This orientation towards consumerism (which also excludes potential sources of nuisance) is neither conducive to encounters and debate nor to political participation (Lofland, 1998). This means that key functionalities

of public space, sociability and political participation, are hindered. In this sense, Patton (2000, p. 181) asked, what is at stake besides privacy when it comes to surveillance of public space. 'How does protecting privacy in public places fail to address the social and cultural significance of public places? People do not value public places for protecting privacy. Rather, public places provide a basis for informal sociality and civic life' (Patton, 2000, p. 181). Patton was onto something. However, his narrow perception of privacy did not allow him to realise that in the context of networked surveillance and privacy in public space, privacy and public space have a functional relationship. On the one hand, privacy also serves to protect those aspects of public space connected to political participation and sociability. And, on the other hand, if certain aspects of public space are protected, then opportunities for achieving privacy in public space will also be preserved. In other words, privacy and public space go hand in hand.

In the next Section I will examine whether the right to respect for private life in Article 8 of the European Convention on Human Rights (ECHR) protects privacy in public and, if so, based on what reasoning and to what extent. Following that examination, I will finally be equipped to answer the question, whether the values, dimensions and mechanisms of privacy in general broadly fit, warrant and enable the protection of privacy in public space or whether other conceptualisations should be created. And, if not, as is indeed the underlying assumption in the dissertation, how should privacy in public space in the context of surveillance within smart cities and living labs, be conceptualised?

6

THE RIGHT TO RESPECT FOR PRIVATE LIFE IN PUBLIC IN THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS*

* For the purpose of clarity, this Chapter uses both in-text references (for literature) and footnotes (for case law and additional explanation).

1. INTRODUCTION

As I have shown in the previous Chapter based on the *Stratumseind Living Lab* (*SLL*) example, there are plenty of privacy and privacy-related risks in public space – for individuals but also for society more broadly. The claim that there are very limited (or none at all) privacy interests in public space, however, persists both in lay (including journalistic) and some theoretical discussions (e.g. Reamer Anderson, 2012). Governments and law enforcement have a vested interest in keeping privacy interests out of public space, as such space is fertile ground for data capture (Kaminski, 2015; Newell, 2018).[183] As do businesses – just think of the companies involved in the *SLL*, whose business models rely on data captured from public space. National courts, although to differing extents, are reserved in both recognizing and protecting the right to privacy in public space. This is not particularly surprising, as such a distinction can still be found in many laws, particularly criminal codes.[184] Even when national courts do recognise such a right, this right seems to commonly 'loose' when balanced against a competing (societal) interest, such as the protection of property or prevention of crime and disorder (Nissenbaum refers to this as the 'knock-down' objection; 1998, p. 571; cf. Picard, 1999).[185] However, the scope of the constitutional protection of privacy in public spaces in several European states is said to be more generous than in US constitutional law, with Canada somewhere in between (Jonsson Cornell, 2016; cf. Boa 2007). This might be connected to the fact that the European Court of Human Rights (ECtHR or the Court) has been a leading force in the field, gradually expanding the scope of the right to respect for private life in Article 8 to – in principle – cover public spaces, certain activities occurring there, and the data incurred from them, already for decades.

183 See, for example: Kravets, D. (2010, September). Feds: Privacy Does Not Exist in "Public Places." *Wired*.

184 See e.g. Chapter 4, Sections 6 and 9 of the Swedish Criminal code criminalising secret recording of images of persons and secret eavesdropping and recording of conversations in a home or another private place. Similar provisions are found in Sections 5 and 6 of the Finnish Criminal Code. A similar provision concerning secret recording of images can be found in Art. 264 of the Danish Criminal Code. A similar provision concerning interception of communications limited to private premises is found in Art. 161-A of the Chilean Criminal Code.

185 This can be seen, for instance, in recent a decision by the Slovenian Higher Court in Maribor (III Kp 37867/2017; para. 6), where the Higher Court acknowledged the existence of a right to privacy in public space but pointed out that such a right is not absolute and that balanced with opposing interests (protection of property in this case), video surveillance of the public space was a legitimate intrusion into this right.

The Court has achieved this through a certain unwillingness to define the right to private life, coupled with an evolutive or 'dynamic and broad' reading of the provision. This evolutive reading reflects both the 'living instrument' approach (Letsas, 2013; Rainey et al., 2017, p. 77)[186] to the European Convention on Human Rights (ECHR or the Convention), as well as the multifaceted nature of privacy. Such an approach to human rights law, while prone to criticism (e.g. Feldman, 1997; Mahoney, 1990), nevertheless allows for the development of the Convention and of Article 8 in accordance with the growing demands of social and, particularly, technological change (Harris, O'Boyle, & Bates, 2018, pp. 361–371). In view of new communication technologies that allow for continuous capture, storage and dissemination of personal data, the Court thus asserted in von Hannover v Germany: 'increased vigilance in protecting private life is necessary'.[187] Indeed, this is a prerequisite of effective protection, as the Convention is 'intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective'.[188] The Court's position that the notion of private life in Article 8 includes 'social' and even some 'public' aspects of one's life, is thus essential for the protection of one's privacy, intrusions into which increasingly happen with the use of new surveillance technologies deployed in public space, particularly with the spread of smart cities and living labs. After several decades of case law, most notably in the last twenty years, it has become firmly acknowledged that the concept of private life from Article 8(1) ECHR may be concerned in measures effected outside a person's home or other private premises.

The values and principles underpinning the Court's analysis of Article 8 suggest that the right to respect for private life is premised upon something else than any *ad hoc* designation of places as private. Quite the contrary, the ECtHR jurisprudence suggests that there is great awareness of the role that privacy plays in the development of an autonomous self and in one's relationships with others. The two crucial concepts that have allowed the Court to widen the scope of the notion of 'private life' in Article 8(1) ECHR beyond a narrow spatial interpretation of the right to privacy, are thus found particularly in 'the right to establish and develop relationships with others and the outside world' and 'the protection of personal data' (Vermeulen, 2014). The use of

186 According to Rainey, Wicks and Ovey (2017, p. 77), the Court has used this notion in about thirty cases. It first used it in the Tyrer v. United Kingdom (1978) App no 5856/71, stating: 'The Court must also recall that the Convention is a living instrument which … must be interpreted in the light of present-day conditions. In the case now before it the Court cannot but be influenced by the developments and commonly accepted standards in the penal policy of the member States of the Council of Europe in this field'.

187 *von Hannover v. Germany* (2004) Application no. 59320/00, § 70.

188 *Ibid*., § 71.

these two concepts has led the Court to recognise a protected zone of interaction of a person with others, even in a public context in a number of cases.[189] More recently, the Court has gone even further, introducing a new – or at least newly named – notion guiding the interpretation of private life – the 'right to lead a private social life' in the 2017 Bărbulescu v. Romania judgment.[190] With the use of these guiding principles (or rights, as the Court sometimes refers to them), the ECtHR has managed not to lock its case law into a public-private distinction, understood as binary opposition.

The aim of this Chapter is *to examine whether the right to respect for private life in Article 8 of the European Convention on Human Rights (ECHR) protects privacy in public and, if so, based on what reasoning and to what extent.*

In order to answer this question, I will examine the case law of the ECtHR, focusing the analysis on the general right to respect for private life, however, relevant discussion in regard to the rights to respect for the home and for correspondence is also included. As the Court itself generally employs the notions of the private and the public *sphere*, rather than referring to – more narrowly – public and private *space*, I also talk about the 'right to respect for private life in public' (that is, in the public sphere), rather than the right to respect for private life in public *space*. As discussed in Chapter 4, the public sphere is commonly defined as the sphere in which private individuals come together as a public in order to engage in – essentially face-to-face – public and critical use of reason (Habermas, 2015, p. 27; for more see Section 3.2 in Chapter 4). In relation to the public sphere, public *space* thus plays a powerful role in the social and political *activities* involved in 'making of the publics' by providing the material space to engage in political participation. Of course, nowadays members of the public commonly meet and publicly communicate through digital technologies as well, resulting in a storm of *data*. Broadly in line with this perspective, the Court examines not only the *space* of the intrusion but also the type of *activity* and, increasingly, the type of *data* that is related to the intrusion.

Following the Court's approach, I have selected Article 8 case law based on a certain connection with 'publicness'. This includes cases in which the interfering measure

189 *Peck v. UK* (2003) Application no 44647/98; *von Hannover v. Germany* (2004); *Bărbulescu v. Romania* (2017) Application no. 61496/08; *Gillan and Quinton v. UK* (2010) Application no. 4158/05, § 6; *Pretty v. UK* (2002) Application no. 2346/02, § 61; *Vukota-Bojić v. Switzerland* (2016) Application no. 61838/10, § 62.

190 *Bărbulescu v. Romania* (2017), § 70; although the right to lead a private social life can already be found in the second section judgment in the case of *Boulois v. Luxembourg* (2010) Application no. 37575/04. However, the Grand Chamber, which decided finally on the case in 2012 did not refer to the right.

has taken place in public space (or at least outside the home), the activity in question was a public or publicly observable activity and/or the data in question had somehow materialised from the 'public domain'.[191] In order to achieve the aim of this Chapter, I have employed a tripartite structure following these elements of publicness – space, activity and data, which echoes the three main categories or themes found in the Court's Article 8(1) assessment of the scope of the right to private life in public. Another reason for settling on this tripartite structure in the first part of the Chapter (Article 8(1) assessment), is the vast scope of the right, which makes it very difficult to find a good classification of cases.[192] Moreover, the Court itself uses its key guiding principles or rights – the right to develop one's identity and personality, the notion of autonomy, the right to establish and develop relationships with other human beings and the outside world, and the protection of data relating to private life – in various types of cases before it, including cases of secret surveillance, search and seizure of the workplace, stop and search powers, publication of one's image or other data relating to private life, and so on. Often, the cases cited in a particular judgment also bear little resemblance to the case under consideration. Consequently, I think that the chosen structure will lead to better clarity in regard to the scope of the right to respect for private life in public as developed in Article 8(1) case law. However, in regard to the analysis of the Article 8(2) assessment, I will abandon this structure. An analysis of the requirements for an intrusion into the right to respect for private life in public as well as the balancing test done in the examination of the state's positive obligations, namely requires an eye for the particularities of the case.

191 I searched the HUDOC database (https://hudoc.echr.coe.int/eng#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}) in February 2018 (with several subsequent searches, the latest on 21 June 2019). Six terms were entered in isolation: 'public space', 'public place', 'public action', 'public activity', 'public data' and 'public information', each with Article 8 as a limiter. Two databases were searched: admissibility decisions and court judgements. This resulted in 84 judgments, which I narrowed down by sifting through them using with the general context of the topic in mind, to 43. Secondly, I employed a snowballing approach – I examined cases referred to in relevant paragraphs of the case at hand, including a few cases relating to Articles 10 and 11. This finally resulted in 65 cases (these are listed in the Literature section).

192 There have been plenty of attempts at a categorisation but none of them is without criticism. Moreham (2006), for example, distinguishes five sub-categories of the private life interest. First, she identifies three 'freedoms from': the right to be free from interference with physical and psychological integrity, from unwanted access to and collection of information, and from serious environmental pollution. Second, she identifies two 'freedoms to': the right to be free to develop one's personality and identity and to live one's life in the manner of one's choosing. These categories, however, significantly overlap and, moreover, do not offer a good structure in the case of the aim of this Chapter, which fits better following the tripartite structure based on the three key categories the Court employs in this context: space, activity and data.

The structure of the Chapter is the following. First, I examine how the Court goes beyond the public-private distinction as a simplistic binary spatial opposition (generally in line with insights from urban geography; see Chapter 4), in particular by (1) recognising the right to establish and develop relationships with others and the outside world, (2) the right to develop one's personality, and (3) limiting the importance of a 'reasonable expectation of privacy' standard in this context. Adopting the tripartite structure, I then review the scope of the right to respect for private life in public. I begin by analysing the scope of the right beyond the home and private premises, focusing on private life in public *space*. After that, I examine which types of *activities* in public space can fall under the scope of Article 8(1) ECHR. And finally, I examine, which types of *data* that have materialised from the public domain, and in which contexts, can fall within the scope of the right to respect for private life. Leaving the tripartite structure behind, I then examine the requirements that may justify an intrusion by public authorities into the right to respect for private life (Article 8(2) assessment) and the state's positive obligations regarding intrusions done by private actors. In my concluding section, I offer some thoughts on future developments of the right to private life and a brief application of the insights gathered from this assessment of ECtHR case law concerning the right to respect for private life in public to the *Stratumseind Living Lab* (*SLL*). I use the *SLL* as an illustrative contemporary example of the proliferating surveillance in public space within contemporary smart cities and examine whether the extent and manner in which this technology is employed, at least in this case, would potentially amount to an interference with Article 8 (or not) and, if so, if it would be considered justified.

2. BEYOND THE PUBLIC-PRIVATE DISTINCTION AS A BINARY OPPOSITION

The undisputed difficulties involved in defining the individual's 'private life' (that is, privacy) have led to it often being explained in binary or exclusionary opposition to 'public life' (see Chapter 4). The individual's private life thus represents 'everything that is not his public life,' that is, a person's 'life in the community, the life which in the normal way brings him into contact with his fellows: his professional and social life, in a word his outside life' (Martin 1959, p. 230; as quoted in Velu, 1973, p. 30). As a result of this persistent distinction, oftentimes understood in a simplistic manner as

a binary opposition between private and public spaces (and sometimes activities),[193] law enforcement, businesses and even courts often perceive the use of surveillance technologies in public space as a more or less harmless endeavour. In fact, earlier case law of the ECtHR (or ECmHR)[194] understood the right to respect for private life in Article 8 as encompassing only a narrow, inner circle of life.[195] As the ECmHR stated in Bruggeman and Scheiten v. Germany: '[A]s earlier jurisprudence of the Commission has already shown, the claim to respect for private life is automatically reduced to the extent that the individual himself brings his private life into contact with public life or into close connection with other protected interests.'[196] The right in Article 8 thus focused on intimate activities and was largely based on a distinction between private and public *space*, where the home was seen as the ultimate private space that required legal protection. In this, the Court seemed to follow the traditional position in privacy law, which saw the home as the centre of private life, 'a zone of immunity to which we may fall back and retreat, a place where we may set aside arms and armor needed in the public place, relax, take our ease, and lie about unshielded by the ostentatious carapace worn for protection in the outside world. This is the place where the family thrives, the realm of domesticity; it is also a realm of secrecy' (Duby, 1987, p. viii).

This persistent approach, which sees the public-private distinction as a binary opposition (primarily between public and private space, but also between private and public activities or data), is still commonly found in positions of governments in the Court's case law and some dissenting opinions of ECtHR judges (e.g. Russian judge Dedov in Khmel v. Russia)[197]. For example, the German government in Niemietz v. Germany maintained that Article 8 did not afford protection against the search of a lawyer's office, since, '[i]n their view, the Convention drew a clear distinction between private life and home, on the one hand, and professional and business life and premises, on the other.'[198] Similarly, the United Kingdom (UK) government argued

193 A binary opposition is a pair of related terms or concepts that are opposite in meaning. In fact, the opposing classes must be mutually exclusive – that is, membership in one class must make impossible membership in the other (Baldick 2001, p. 27).

194 From 1954 to 1998 (when Protocol 11 of the ECHR came into force), individuals did not have direct access to the Court; they had to apply to the Commission (ECmHR), which if it found the case to be well-founded would launch a case in the Court on the individual's behalf. Protocol 11 abolished the Commission, enlarged the Court, and allowed individuals to take cases directly to it.

195 *X v. UK* (1973) Application no. 5877/72; *Friedl v. Austria* (1994) Application no. 28/1994/475/556.

196 *Bruggeman and Scheiten v. Germany* (1976) App. 6959/75, DR vol. 10, p. 100.

197 *Khmel v. Russia* (2014) Application no. 20383/04, p. 21.

198 *Niemietz v. Germany* (1992) Application no. 13710/88, § 27.

in Perry v. UK, that the filming in the custody area of a police station did not take place in a private place, so that there could not be any intrusion into the 'inner circle' of the applicant's private life.[199] In the S.A.S. v. France case, the French government submitted that Article 8 does not apply, since the ban on clothing designed to cover the face concerned only public places, so that it could not be considered that an individual's physical integrity or privacy were at stake.[200] In the recent Antović and Mirković v. Montenegro case concerning video surveillance of university halls, the Montenegrin government argued that the surveillance took place in public and could thus not be considered to be an interference with Article 8, unless it was disclosed or published.[201] Similarly, in Khmel v. Russia, the Russian government argued that after the applicant has committed a breach of public order, caused damage to the honour and dignity of the authorities and had been escorted to the police station, his private life has been brought into the public domain.[202]

Similar claims relating to public *activity* and *data* (or information) are found in other cases. For example, in P.G. and J.H. v. the UK, the UK government held that use of listening devices in the cells and when the applicants were being charged did not disclose any interference, as the recordings were not made to obtain any private or substantive information.[203] Furthermore, '[t]he aural quality of the applicant's voices was not part of private life but was rather a public, external feature'.[204] Similarly, the Romanian government in Rotaru v. Romania, claimed that Article 8 was not applicable since the information in the secret services file on the applicant related to his public life: 'By deciding to engage in *political activities* and have pamphlets published, the applicant had implicitly waived his right to the "anonymity" inherent in private life. As to his questioning by the police and his criminal record, they were *public information*.'[205]

Contrary to these common claims in the positions of governments, the Court has, at least since the 1990s, moved away from this position and begun to state that the right to respect for private life extends beyond the private family circle and includes a social

199 *Perry v. UK* (2003) Application no. 63737/00, § 33.

200 *S.A.S. v. France* (2014) Application no. 43835/11, § 84.

201 *Antović and Mirković v. Montenegro* (2018) Application no. 70838/13, § 50.

202 *Khmel v. Russia* (2014) Application no. 20383/04, § 38.

203 *P.G. and J.H. v. the UK* (2001) Application no. 44787/98, § 54.

204 *Ibid*.

205 *Rotaru v. Romania* (2000) Application no. 28341/95, § 42; emphasis added.

dimension.[206] The fact that the Court did not define the scope of the right to private life in a simplistic binary opposition to 'public life' can most clearly be seen in the by now classic 1992 Niemietz judgment.

In this judgment, the ECmHR argued that professional activities *could* fall within the scope of the right to respect for private life, however, noting that 'whether or not such matters have to be considered as relating to a person's private sphere, *as opposed to public life*, depends upon the relevant features of the *activities* and *premises* concerned'.[207] The Commission here understood privacy as confidentiality of communications, seeing it as a necessary requirement in order to preserve the trust within the privileged lawyer-client relationship. The Court, however, expressly did not follow this reasoning. It offered doubts as to whether the confidential relationship between a lawyer and a client could serve as a workable criterion for the purposes of delimiting the scope of the protection afforded by Article 8. 'Virtually all professional and business activities may involve, to a greater or lesser degree, matters that are confidential, with the result that, if that criterion were adopted, disputes would frequently arise as to where the line should be drawn'.[208]

Furthermore, the Court asserted that it is not always possible to distinguish clearly which activities of an individual form part of her professional or business life and which do not. This assertion of the ECtHR could thus be seen as noting that the precise location of the dividing line between what is public and what is private goes beyond simplistic exclusionary distinctions between (more or less arbitrary) designations of 'public v. private space' or 'private v. public actions'. Instead, these are heavily contested divisions, a fact with which binary models struggle enormously. The Court continued:

> '(…) especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time. To deny the protection of Article 8 on the ground that the measure complained of related only to professional activities – as the Government suggested should be done in the present case – could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so

206 *Niemietz v. Germany* (1992), § 29; *Shimovolos v. Russia* (2011), § 64; *von Hannover v. Germany* (2004), § 69; *von Hannover v. Germany (no. 2)* (2012) Applications nos. 40660/08 and 60641/08, § 50.

207 *Niemietz v. Germany* (1992), § 56; emphasis added.

208 *Ibid*., § 28.

> intermingled that there was no means of distinguishing between them. In fact, the Court has not heretofore drawn such distinctions …'[209]

Crucially, the Court held that it would be too restrictive to limit the notion of 'private life' to an 'inner circle' – restricting it to a *private space* (the home), in which the individual may perform the most *private or intimate activities* and make personal choices – and to exclude therefrom entirely the outside world not encompassed within that circle.[210] Instead, the Court posited that one of the main purposes of the right to private life protects the right to establish and to develop relationships with other human beings. Significantly, it found that there is no reason or principle why this broad understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since the majority of people have a significant, if not the greatest, opportunity to developing relationships with the outside world precisely in the course of their working lives.

With this influential early judgment, the Court opened the door to the recognition of a 'zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[211] The Court thus managed not to lock itself into a binary public-private distinction in its Article 8 case law, as I will show in more detail in the following sections (see Sections 3, 4 and 5). This means that the scope of the right to private life is, in principle, not limited by the nature of the premise in which the intrusion takes place, or even to the nature of the activity or data, thus allowing for a right to respect for private life in public. The relevant distinction that the Court employs thus is not between a 'private and a public *space*' but a 'private and public *sphere*', where a person's private sphere is understood in a broad manner and at a variety of scales that overlap and intersect (see Chapter 4).

In the following sub-sections, I will briefly examine the main principles (or rights) that guide the Court's interpretation of the scope of Article 8(1) and are of particular importance when it comes to the right to private life in public: the right to establish and develop relationships with others and the outside world, the right to protection of one's image and the reasonable expectation of privacy standard.

209 *Ibid*., § 29.

210 *Ibid*., § 28.

211 *Peck v. the UK* (2003), § 57; *P.G. and J.H. v. UK* (2001), § 56; *Uzun v. Germany* (2010) Application No. 35623/05, § 43; *Perry v. UK* (2003), § 36; *Niemietz v. Germany* (1992), § 33-34; *Halford v. UK* (1997) Application no. 20605/92, § 44; *Vukota-Bojić v. Switzerland* (2016), § 52; *Köpke v. Germany* (2000) no. 420/07.

2.1 The right to establish and develop relationships with others and the outside world: the right to lead a 'private social life'

One of the key principles that guide the interpretation of the scope of Article 8 and the one that is of most importance for the right to respect for private life in public is 'the right to establish and develop relationships with others and the outside world'. While the Court acknowledged that everyone *indeed* has the right to live privately, away from unwanted attention,[212] this does not mean that the notion of 'private life' is limited to an 'inner circle' in which an individual may live her or his own personal life as she chooses, thus excluding the outside world not encompassed within that circle.[213] Private life, the Court declared in X v. Iceland in 1976, extends to relationships with other persons, which are necessary for the 'development of his personality'.[214] Since then the Court has repeatedly stated that one of the key elements of the right to respect for private life is the right to establish and develop relationships with others and the outside world, which leads to a zone of interaction with others even in a public context.[215]

Building on this right, the Court introduced a new phrasing of the right (potentially broadening its scope) in the 2017 Bărbulescu judgment, a case concerning extensive monitoring of online communications at the workplace. In this case the Court stated: 'Article 8 thus guarantees a right to "private life" in the broad sense, including the right to lead a "private social life", that is, the possibility for the individual to develop his or her social identity.'[216] The Court further briefly explains that this right *enshrines* the possibility of approaching others in order to establish and develop relationships with them.[217] The Court also observed that internet instant messaging services, such as *Yahoo Messenger*, which was the means of communication in this case, is just one of the many possible forms of communication enabling individuals to lead a private social life. The Court concluded that

212 *Smirnova v. Russia* (2003) Applications nos. 46133/99 and 48183/99, § 95.

213 *X v. Iceland* (1976) App. 6825/74, Decisions and reports [DR], vol. 5.

214 *Ibid*., p. 87.

215 *Peck v. UK* (2003); *von Hannover v. Germany* (2004); *Bărbulescu v. Romania* (2017); *Gillan and Quinton v. UK* (2010); *Pretty v. UK* (2002).

216 *Bărbulescu v. Romania* (2017), § 70.

217 Referring to cases: *Bigaeva v. Greece* (2009) Application no. 26713/05, § 22; Özpinar v. Turkey (2011) Application no. 20999/04, § 45 *in fine*.

> '[b]e that as it may [regarding the reasonable expectation of privacy], an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary'.[218]

In a succession of recent cases concerning surveillance at the workplace, confidential communications with a lawyer[219] and even in the context of anti-doping testing,[220] the Court has confirmed the 'right to lead a private social life'.[221] In these cases the Court held that restrictions on an individual's life in public context (including one's professional life) may fall within Article 8, where they have repercussions on the manner in which one constructs one's social identity by developing relationships with others. While this notion was developed in the context of workplace surveillance, it has since been applied to other contexts as well. Moreover, it clearly builds on the existing ECHR right to establish relationships with others and the outside world, which has been used in a variety of earlier cases concerning Article 8. Consequently, one might imagine the value of the notion of 'the right to a private social life' in relation to public spaces and even public activities, as persons develop their social identity also in the context of public life, participating in public space and public activities (indeed, this is suggested in FNASS and Others v. France; I discuss this further in Sections 4 and the Conclusion).

218 *Bărbulescu v. Romania* (2017), § 80.

219 Article 8 'encompasses the right for each individual to approach others in order to establish and develop relationships with them and with the outside world, that is, the right to a "private social life", and may include professional activities or activities taking place in a public context (see Bărbulescu v. Romania [GC], no. 61496/08, §§ 70-71, 5 September 2017). There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see Uzun v. Germany, no. 35623/05, § 43, ECHR 2010 (extracts) with further references). The Court further considers that a person's communication with a lawyer in the context of legal assistance falls within the scope of private life since the purpose of such interaction is to allow an individual to make informed decisions about his or her life. More often than not the information communicated to the lawyer involves intimate and personal matters or sensitive issues'; Altay v. Turkey (no. 2) (2019) Application no. 11236/09, § 49.

220 The case concerned the possibility of anti-doping checks to be carried out during sports events, training periods and other periods of time that were independent of the athlete's competition or training time. As such, the location of the testing could essentially take place at any location with the permission of the athlete, requiring them to give detailed daily schedules for the coming trimester, including one-hour slots per day during which they will be present in a certain location to enable unannounced checks.

221 *Antović and Mirković v. Montenegro* (2018), § 41; *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France* (2018) Applications nos. 48151/11 and 77769/13, § 153.

2.2 Protection of one's image

Another essential component of the right to personal development is the right to protection of a person's image against unwanted recording, which extends – at least to a certain extent – to public spaces as well. A persons' image is considered one of the 'essential components of personal development', as it reveals the person's unique characteristics and distinguishes the person from his or her peers.[222] As such, it mainly presupposes the right to control the use of that image, including the right to refuse publication thereof but it can also cover the right to object to the recording as such. As the Court stated in Reklos and Davourlis v. Greece, a case about photographing a new-born in a private clinic without the consent of the parents:

> 'Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person. As a person's image is one of the characteristics attached to his or her personality, its effective protection presupposes, in principle and circumstances such as those of the present case […] obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published. Otherwise an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image.'[223]

This assessment is, of course, further influenced if the person involved is a public figure or not. Politicians, for example, 'inevitably and knowingly lay themselves open to close scrutiny by both journalists and the public at large'.[224] These public figures *par excellence* first need to be distinguished from 'relatively' public figures, like the princess von Hannover, that are open to a lower level of scrutiny to the public.[225] The image of persons who are not public or newsworthy figures at all (that is, 'ordinary persons'), however, cannot be recorded without their knowledge or consent.[226] Furthermore, it is not required that the pictures show a person in a state that could be regarded as degrading, or in general as capable of infringing his personality rights.[227] A bigger issue will be whether the photographer retains the images and negatives, allowing

222 *López Ribalda and others v. Spain* (2018), § 56; *von Hannover v. Germany* (no. 2) (2012), § 96; *Reklos and Davourlis v. Greece* (2009) Application no. 1234/05, § 40; *Khmel v. Russia* (2014), § 40.

223 *Reklos and Davourlis v. Greece* (2009), § 40.

224 *Craxi v. Italy* (2000) Application no. 25337/94, § 64.

225 *von Hannover v. Germany* (2004), § 73.

226 *Reklos and Davourlis v. Greece* (2009), § 41.

227 *Ibid*., § 42.

for reproduction and dissemination, without the person's consent, so that the image of a person is retained in the hands of the photographer in an identifiable form with the possibility of subsequent use against the wishes of the person concerned.[228] Based on this distinction between public figures *par excellence*, relative public figures and 'ordinary persons', the Court has confirmed that ordinary persons enjoy an enlarged the zone of interaction even in a public context that may fall within the scope of private life protected in Article 8.[229]

2.3 The limited importance of a reasonable expectation of privacy

In the context of ascertaining whether the notion of 'private life' is applicable in a certain case, the Court has on several occasions, particularly in relation to privacy in public, used the standard of a 'reasonable expectation of privacy'.[230] It has done this in a somewhat confusing and incoherent manner, sometimes referring to standard by a different name, either as a 'legitimate expectation of privacy'[231] or whether or not the intrusion was 'foreseeable'.[232] While these tools are reminiscent of those used in common law jurisdictions, the Court uses the standard(s) in a somewhat haphazard fashion and has not developed it into a concrete test for application of the Convention right (Gómez-Arostegui, 2005).[233] This standard originating in common law jurisdictions has been mentioned mostly in cases against the UK, occurring first in cases of surveillance of communications at the workplaces[234] and then spreading also to other cases concerning surveillance, searches in the workplace and the use of police powers in public space.

The second case in which the Court used the reasonable expectation of privacy standard, is the case of P.G. and J.H v. UK.[235] It concerned the covert recording of a conversation between a police officer and a suspect in order to obtain an audio sample of the suspect's voice, making it possible to identify conspirators and prevent a robbery. In this early case, the Court stated its approach to the standard, which seems

228 *Ibid*., § 42-43; also *P.G. and J.H. v. UK* (2001), § 57.

229 *Sciacca v. Italy* (2005) Application no. 50774/99, § 29.

230 *Halford v. UK* (1997), § 44-45; *Peev v. Bulgaria* (2007) Application no. 64209/01, § 39; *Niemietz v. Germany* (1992).

231 *von Hannover v. Germany* (2004).

232 *Peck v. UK* (2003).

233 For a more detailed discussion on the application of the test (in particular, subjective and objective expectations of privacy), see Gómez-Arostegui (2005).

234 *Halford v. UK* (1997).

235 *P.G. and J.H. v. UK* (2001).

to still hold today – that is, that the reasonable expectation of privacy is not the sole or primary basis when determining whether an intrusion into private life has occurred; instead, it is one of several factors that the Court considers.

> 'There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, *a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive factor*.'[236]

In particular, the Court stressed another factor – whether and how personal data concerning the applicants is processed: 'Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain'.[237] The Court reached similar conclusions in Perry v. UK[238] and Peck v. UK,[239] both cases concerning surveillance in a type of public space (a police station and a public street). In none of the cases, however, does the Court clearly explain how these factors relate to each other; they might be considered as separate factors, or the reasonable expectation of privacy might be applied as a part of the processing of personal data factor.

236 *Ibid*., § 57; emphasis added.

237 *Ibid*.

238 In the case of *Perry v. UK* (2003), for example, the police regulated the security camera in the police station in such a way that it could take sharper footage of the applicant and inserted it in a montage of film of other persons to show witnesses for the purpose of seeing whether they would identify the suspect under investigation. The montage was also shown during the applicant's trial in a public court room. The Court found that there was no indication that the applicant had any expectation that footage was being taken of him within the police station for use in these specific ways (*ibid*., § 41). As such, this 'ploy' by the police went beyond the normal or expected use of this type of camera in the police station (*ibid*.). However, the Court also considered another relevant factor when determining whether an interference has occurred – the fact that the recording and subsequent use in a montage resulted in the collection and processing of personal data.

239 The Court conducted a similar analysis in *Peck v. UK* (2003), where Peck was filmed by CCTV holding a knife in public space. The Court considered that the key element in this case, was the fact that there was a disclosure of the footage and pictures (via television and the press), which revealed Peck's identity (his face was either poorly masked or not at all) and actions to the public in a manner, which he could not have foreseen. 'As a result, the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation … and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995 (*ibid*., § 62).

While the Court has not yet offered a clear stance towards the standard of a reasonable expectation privacy, more recent case law concerning surveillance at the workplace might suggest that the standard holds less weight than some other factors, at least in this context. In Bărbulescu v. Romania, a case concerning surveillance of online communications at the workplace, the Court noted that the applicant had been informed of the ban on personal internet use in the employer's internal regulations.[240] It had not been convinced, however, that he was informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications. The Court stated that '[i]t is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy.'[241] Moreover, it concluded that *'[b]e that as it may, an employer's instructions cannot reduce private social life in the workplace to zero*. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary'.[242] This suggests that even a detailed and clear full prohibition of the use of internet at the workplace for personal matters given in advance, for example, cannot reduce this right to zero. This position, which considers 'the right to lead a private social life' as having more weight than a reasonable expectation of privacy has been confirmed in a subsequent judgment, Antović and Mirković v. Montenegro, a case concerning surveillance in university auditoriums.[243]

It remains unclear how the Court might use the standard in other cases and contexts. What can be said, however, is that the Court does not seem to use this standard (in any of its various forms) to delineate the scope of the right to respect for private life on its own (Gómez-Arostegui, 2005, p. 162), rather it uses it as one factor among others. As such, the reasonable expectation of privacy can be seen as a heuristic tool occasionally used to give more or less weight to certain other factors. While this matter merits a more detailed discussion, I conclude here that this might in fact be a desirable outcome. The reasonable expectation of privacy standard as found in common law jurisdictions, namely, faces significant challenges. It is an inherently subjective process, depending on the judges' understanding of the implications of the

240 *Bărbulescu v. Romania* (2017), § 77-78.

241 *Ibid*., § 80.

242 *Ibid*.; emphasis added.

243 *Antović and Mirković v. Montenegro* (2017), § 44; 'Furthermore, the Court has also held that even where the employer's regulations in repsect of the employees' private social life in the workplace are restrictive they cannot reduce it to zero' (*ibid*., § 44). In this case, the Court also noted the factor of processing of personal data as relevant.

facts of a given case, and the relationship of those facts to their understanding of the nature and value of privacy (Boa, 2007, p. 330). Furthermore, the idea of 'expectations' is closely tied to social conventions and practices. Yet, simply because a particular practice comes into existence (especially through the quick development and even quicker deployment of a new technology) and individuals have come to expect it, this does not necessarily mean that it there is no privacy interest left (*ibid*., p. 332). As Cohen (2017, p. 461) put it, 'reasonable expectation is precisely the problem', as it instils an expectation of being surveilled, thus normalising the disciplinary effects of surveillance. Therefore, by not limiting its analysis to this standard, the ECtHR does not lock itself into a paradoxical situation, where pervasive but conspicuous and thoroughly notified surveillance would limit persons' privacy to a negligible level. This is particularly relevant for contemporary public space in its transformation into smart cities.

3. BEYOND THE HOME: WORKPLACE AND PUBLIC SPACE – ZONES OF INTERACTION EVEN IN A PUBLIC CONTEXT

Earlier ECtHR (or ECmHR) case law seems to have limited the scope of the right to respect for private life to private premises by continuing to expressly refer to the fact that the intrusion did not take place within the home. In the early case of X v. UK from 1973, for example, the Commission dismissed the notion that the making of and retention of a photograph of an individual in a public space could interfere with the right to private life, finding the application of Ms. X manifestly ill-founded.[244] The case concerned Ms. X who attended a rugby match in 1969 and joined a number of people on the pitch in a peaceful demonstration against the South African government's apartheid policy. Ms. X was later forcibly restrained by the police and photographed against her will. The police retained the negatives and copies of the mentioned photos and refused to destroy the photos. The Commission did not consider this an interference with the private life of Ms. X for three reasons: (1) there was 'no invasion of the applicant's privacy in the sense that the authorities entered her home and took photographs of her there'; (2) 'the photographs related to a public incident in which she was voluntarily taking part'; and (3) the photographs were taken 'solely for the purpose of her future identification on similar public occasions and there is no

244 *X v. UK* (1973) Application no. 5877/72.

suggestion that they have been made available to the general public or used for any other purpose'.[245]

The argumentation was very similar in the case of Lupker and others v. the Netherlands from 1992, in which the Dutch police investigated a fire at the Town Hall in Nijmegen.[246] In order to find the perpetrators, the police used a book containing photographs of suspects (a group of squatters/protesters that had been removed from an office building in Nijmegen by the police just days before), which they showed only to potential witnesses. These photographs had either been given to the authorities in connection with applications for a passport or driving licence or had been taken by the police in connection with previous arrests. The Commission did not consider this to amount to an interference with Article 8, giving three similar reasons as in X v. UK: (1) the photographs 'were not taken in a way which constitutes an intrusion upon the applicant's privacy'; (2) the photographs were 'kept in police or other official archives since they had been either provided voluntarily … or taken by the police in connection with a previous arrest'; and (3) they were used 'solely for the purpose of the identification of the offenders in the criminal proceedings against the applicants and there is no suggestion that they have been made available to the general public or used for any other purpose'.[247] While not expressly referring to the home in the first factor, it is clear from the facts of the case and the following factors that what is meant here is that the photographs were not taken in a private place or during a private or intimate activity. The second factor, at least in relation to pictures taken during a previous arrest, also suggests that the photographs constitute data in the public domain (discussed in Section 5). In earlier ECtHR case law, one can thus observe that the *place of intrusion* was one of three key factors determining the scope of the right to private life.

In later case law of the ECtHR, by relying on broad conceptions of the private and public sphere and, in particular, on the guiding principle of developing relations with others and the outside world, the Court changed its approach and began to expand the scope of Article 8. This began by expanding the right to respect for one's home, first to include residential premises such as holiday homes, hotels providing

245 *Ibid*., 16 Y b, p. 328.

246 *Lupker and others v. the Netherlands* (1992) App. 18395/95.

247 Ibid., § 5, *al*. 4; the admissibility decision is available at: Lupker and others v. the Netherlands. (1992). Retrieved March 28, 2019, from http://echr.ketse.com/doc/18395.91-en-19921207/view/.

long-term accommodation[248] and even caravans,[249] and then beyond purely residential premises, granting protection to lawyers' offices. The expansion of protection beyond residential premises began in 1992 with the Niemietz v. Germany case.[250] In this case, as already discussed above, the Court noted that it is not always possible to draw precise distinctions between a home and a professional office, since activities that are related to a profession or business, may well be conducted from a person's private residence, and activities that are not so related, may well be carried on in an office or commercial premises. A narrow interpretation of notions 'home' and 'domicile' (just like with the notion of 'private life') could therefore give rise to the risk of inequality of treatment. The Court accomplished this interpretation by making clear that the notion of the 'home' in the Convention is an autonomous concept that does not depend on the classification under domestic law. The expansion that followed then came to encompass business premises[251] or a combination of residential and business premises, where there is no clear distinction between a person's office and private residence or between private and business activities,[252] journalists' premises, and desks or filing cabinets of employees.

Importantly, later ECtHR case law on surveillance within the workplace (either within public or private institutions) moved away from considering the workplace as a type of 'home' and instead focused on the question, whether the general notion of 'private life' was involved, increasingly examining it without referring to the right to respect for one's home at all. This move means that the Court does not need to constantly expand the meaning and scope of the 'home' and can extend privacy protection to increasing types of spaces, including public space. In recent cases, such as, Köpke v. Germany[253] and Antović and Mirković v. Montenegro,[254] the Court thus found that video surveillance at the workplace constitutes an interference with the general right to private life (rather than the home), which guarantees a broad level of protection, including the protection of the right to lead a private social life, establishing a zone of interaction with others in a public context, where professional life is a part of it.

248 *Demades v. Turkey* (2003), Application no. 16219/90.

249 *Buckley v. UK* (1996) App 20348/92.

250 *Niemietz v. Germany* (1992).

251 *Wieser and Bicos Beteiligungen GMBH v. Austria* (2007) Application no. 74336/01, §43.

252 *Buck v. Germany* (2005) Application no. 41604/98, § 31.

253 *Köpke v. Germany* (2010).

254 *Antović and Mirković v. Montenegro* (2018), § 42.

The Court very rarely discusses the nature or type of public space in relation to interference with private life. Cases relating to Article 8 in which an intrusion somehow occurs outside of the home or workplace range widely. They relate to multi-purpose and open public spaces such as streets[255] and roads,[256] as well as to semi-public spaces with a dedicated purpose (enclosed or open), such as university halls,[257] storage facilities,[258] private clinics,[259] private beach clubs,[260] police stations,[261] stadiums[262] and shopping centres.[263] Somewhat surprisingly then, in Gillan and Quinton v. UK, a case relating to a stop and search without reasonable suspicion in the street, the Court notes that a distinction between a public street and specific public spaces (or specific zones of public space), such as airports or other public buildings, needs to be made.[264] It noted that while an air traveller may be seen as consenting to a search by choosing to travel, since she knows that her bags are liable to being searched before boarding and thus has freedom of choice to leave behind any personal items, a stop and search without reasonable suspicion in a public street is qualitatively different. According to such stop and search powers, any individual can be stopped anywhere at any time, without notice and without any choice whether or not to submit to a search.[265] The Court thus seems to have distinguished between a multi-purpose public space and a dedicated-purpose public space, which might come with special surveillance needs (in the case of an airport for purposes of security) that do not apply to public space in general.

In this way, the Court confirms that the place of intrusion into one's Article 8, does not necessarily have a negative effect on the determination of the severity of the intrusion, quite the contrary, it can compound the severity of the intrusion. As the Court in Gillan and Quinton stated: 'Although the search is undertaken in a public place, this does not mean that Article 8 is inapplicable. Indeed, in the Court's view,

255 *Peck v. UK* (2003); *Gillan and Quinton v. UK* (2010); *von Hannover v. Germany* (2004); *von Hannover v. Germany* (no. 2) (2012).

256 *Uzun v. Germany* (2010).

257 *Antović and Mirković v. Montenegro* (2018).

258 *Sorvisto v. Finland* (2009) Application no. 19348/04.

259 *Reklos and Davourlis v. Greece* (2009).

260 *von Hannover v. Germany* (2004).

261 *Perry v. UK* (2003).

262 *X v. UK* (1973) App. 5877/72.

263 Mentioned in *Perry v. UK* (2003), § 40.

264 *Gillan and Quinton v. UK* (2010), § 64.

265 *Ibid*., § 64.

the public nature of the search may, in certain cases, compound the seriousness of the interference because of an element of humiliation and embarrassment.'[266] While the case at hand relates to an intrusion into one's physical integrity (a rather minor one, namely, a very superficial personal search), the Court makes these claims in a very general way, which might apply to other types of intrusions into one's private life, such as those intruding solely into one's psychological integrity, as well. This view seems to be confirmed by the Antović and Mirković v. Montenegro[267] and López Ribalda and others v. Spain[268] judgments, in which the Court concluded that covert video surveillance of an employee at her workplace (a dedicated-purpose type of space outside of the 'home') must be considered as a considerable intrusion into the employee's private life, since it entails recorded and reproducible documentation of a person's conduct at her workplace, which the individual cannot evade, as she is contractually obliged to perform the work *in that specific place*. Based on these judgments, one could therefore argue that the more multiple the purposes of use of the space at issue (*ceteris paribus*), the higher the reasonable expectation of privacy, as such space would potentially involve more parts of one's social life and one would not have a real (that is, acceptable) choice to avoid it. This is a particularly valuable takeaway for considering the surveillance of multiple-purpose public space, as in cases of smart cities and living labs.

As the most interesting cases for the topic of this dissertation relate to surveillance of public space (either multiple- or dedicated-purpose) with the use of technology, I will now examine how the Court deals with these cases. The Court held in the 1998 case of Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium that the monitoring of the actions of an individual in a public place by the use of photographic equipment, which does not record the visual data, *does not*, as such, give rise to an interference with the individual's private life.[269] The reasoning behind this decision is that this type of surveillance is comparable to being observed on the street by passers-by, which is a part of the experience of being in public space. This position has been confirmed in later influential judgments, including Peck v. UK,[270] P.G. and J.H. v. UK[271]

266 *Ibid*., § 63.

267 Antović and Mirković v. Montenegro (2017), § 44.

268 López Robalda and others v. Spain (2018), § 59.

269 *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium* (1998) Applications nos. 32200/96 and 32201/96, Decisions and Reports [DR] 92-B, p. 97.

270 *Peck v. UK* (2003), § 59.

271 *P.G. and J.H. v. UK* (2001), § 57.

and Perry v. UK.[272] However, in these later cases the Court further noted that recording of data and the systematic or permanent nature of the record – as is common practice today – *may* give rise to an interference with one's private life.

In the case of Uzun v. Germany, where there was a systematic collection and storage of data that determined a person's whereabouts and movements in public space, leading to the creation of a pattern of the person's movements, an interference with Article 8(1) did arise.[273] In this sense, the Court seems to follow the opinion in privacy scholarship, which distinguishes the exposure in public space by contemporary technologies with their capacity to continuously capture, record and analyse data and limited exposure to the naked eye or to those technologies that do not record or analyse data (Moreham, 2006, p. 617). Therefore, surveillance of public space, which involves *limited* observation by unaided human perception or technology that does no more than what human perception allows for,[274] in itself does not constitute an interference with the right to private life.[275] When the capabilities of the technology, however, exceed those of human perception, such as in the case of recording data, zooming in and pattern recognition, an interference with Article 8 is much more likely and further factors need to be examined.

The Court established several additional factors in more recent case law, which need to be considered (alternatively rather than cumulatively) whether a person's private life is concerned in measures effected outside a person's home or private premises, diverting from the approach in older case law, as in X v. UK and Lupker and others v. the Netherlands, where the space of intrusion carried significant relevance. These factors now include: (1) whether a person knowingly and intentionally involves herself in activities which are or may be recorded in a public manner; (2) a person's reasonable expectation of privacy; (3) whether a systematic or permanent record has been made of such material in the public domain; (4) whether there is a compilation of data on a particular individual; *or* (5) whether there has been processing or use of

272 *Perry v. UK* (2003), § 40.

273 *Uzun v. Germany* (2010), § 51.

274 By unaided human perception I mean the naked human eye but also the use of very low-level 'technology', such as glasses.

275 However, a police officer following someone for days on end and observing everything one does in public, may also infringe privacy, even if technology is not used.

personal data, including the publication of the material concerned, in a manner or degree beyond that normally foreseeable.[276]

This rather copious case law clearly confirms that the right to respect for private life can be intruded upon even when measures are effected outside a person's home or private premises. However, as can be seen from the more recently identified factors, the location of the intrusion is neither the only nor a very relevant factor,[277] when determining whether an interference with one's private life took place. Amongst other factors, two main themes can be identified: the theme concerning the type of activity (whether the activities involved concern public or private behaviour, simply occurring in public space) and the theme concerning the type and context of data (whether the data that is captured within the public domain is personal data or other data that relates to the private sphere, and how such data is subsequently used). I will examine these two themes in the way they determine the scope of the right to respect for private life in public in the following sections.

4. BEYOND INTIMATE AND PRIVATE ACTIVITIES: SCENES FROM A DAILY LIFE

When the Court performs its assessment of whether an interference with private life has occurred, the nature of one's activity – whether public or private – is a factor that commonly prevails over the location of the activity (Vermeulen, 2014, p. 33). While the Court has made it clear in its case law that a measure enacted in public space *can* lead to an interference with Article 8, the Court usually limits this possibility to *private* activities that take place in public.

Earlier ECtHR case law found interferences with one's private life *only* when private activities occurring in public space were involved. This can be seen, in particular, in three cases: X v. UK,[278] (1973), Friedl v. Austria[279] and Herbecq and the Association 'Ligue

276 *Uzun v. Germany* (2010), § 44-45; *Perry v. UK* (2003), § 37-38; *P.G. and J.H. v. UK* (2001) § 57; *Peck v. UK* (2003) § 58-59; *Rotaru v. Romania* (2000) § 43-44; *Vukota-Bojić v. Switzerland* (2016) § 55-56

277 The Court still sometimes refers to the fact that the intrusion did not take place in a private place, such as a private residence or vehicle, as it did in the case of *R.E. v. UK* (2016) Application no. 62498/11, § 159, using this as an additional but minor factor taken in consideration.

278 *X v. UK* (1973).

279 *Friedl v. Austria* (1992).

des droits de l'homme' v. Belgium.[280] In X v. UK, which was described in more detail above, the second relevant factor, which led the Commission to find the application manifestly ill-founded, was that the photographs of Ms. X related to a demonstration – a public incident, in which she was voluntarily taking part.

Similarly, in Friedl v. Austria, Mr. Friedl was photographed in a sit-in demonstration by homeless persons in an underground passage for pedestrians in Vienna. When the police arrived, they asked the participants to disperse because they were obstructing pedestrian traffic. As the protesters did not immediately agree to leave, police officers established their identity and took their photographs in order to record the conduct of the participants in the manifestation for the purposes of ensuing investigation proceedings for offences against the Austrian Road Traffic Regulations. This personal data was then stored in a file by the Vienna Federal Police Department. In this case, the Commission reiterated its reasoning in X v. UK, namely: (1) that there had been 'no intrusion into the "inner circle" of the applicant's private life in the sense that the authorities would have entered his home and took the photographs there'; (2) that the photographs related to a 'public incident' – a manifestation of several persons in a public place – in which the applicant was voluntarily taking part; and (3) that they were solely taken in order to ensuing investigation proceedings for offences against the Road Traffic Regulations.[281] While the Court first noted in both cases, that the interfering measure took place in public space, it also noted that it concerned voluntary participation in a public activity, thus forming a part of one's public life and, hence, not protected by the right to private life.

In Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium, the Commission reiterated these factors again. Besides noting that the visual observation in the case occurred in public or semi-public space in order to monitor the premises for security purposes, the Commission emphasized that the mere monitoring by technological means of 'public behaviour' (without recording any data) does not in itself amount to an interference with the right to private life. In particular, the Commission noted that 'the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person … Therefore all that can be observed is, essentially, public behaviour. The applicant has also failed plausibly to demonstrate that private actions occurring in public could have been monitored

280 *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium* (1998).

281 *Friedl v. Austria* (1992), Report of the Commission, 1994, § 49; Available at: Friedl v. Austria. (1992). Retrieved March 28, 2019, from https://www.menschenrechte.ac.at/orig/94_5/Friedl.pdf.

in any way'.[282] From this early case law, a rough distinction can be discerned between 'public activities' (or public behaviour), encompassing activities that are performed in public usually with others (such as a public protest) and 'private activities', which commonly occur in private space but may also occur in public space.

This position has been confirmed in more recent case law and is reflective of a somewhat more sophisticated public-private distinction permeating Article 8, which distinguishes between a public and a private *sphere* (rather than *space*).[283] Moreover, the Court seems to emphasise a particular factor of public activity – that of voluntary participation in such activities. In relation to demonstrations as a textbook example of a public activity, the Court seems to follow the idea that the main reason for demonstrating is to be seen and heard, in other words, to draw attention to oneself. According to this perspective, the Court is of the opinion that participants in such events should thus expect less privacy, drawing a connection with the standard of a reasonable expectation of privacy.

In Friend and the Countryside Alliance and others v. UK, a case concerning hunting, the Court confirmed that activities, which are of 'essentially public nature' are not protected by Article 8. As it noted: 'There is, however, nothing in the Court's established case law which suggests that the scope of private life extends to activities which are of an essentially public nature'.[284] In this judgment, the Court notes that British fox hunting is – by its very nature – a public activity:

> 'It is carried out in the open air, across wide areas of land. It attracts a range of participants, from mounted riders to followers of the hounds on foot, and very often spectators. Despite the obvious sense of enjoyment and personal fulfilment the applicants derived from hunting and the interpersonal relations they have developed through it, the Court finds hunting to be too far removed from the personal autonomy of the applicants, and the interpersonal relations they rely on to be too broad and indeterminate in scope, for the hunting ban to amount to an interference with their rights under Article 8.'[285]

282 *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium* (1998), DR 92-B, p. 97.

283 *P.G. and J.H. v UK* (2001); *Peck v. UK* (2003); *Friend and the Countryside Alliance and others v. UK* (2009) Applications nos. 16072/06 and 27809/08; *von Hannover v. Germany* (2004).

284 *Friend and the Countryside Alliance and others v. UK* (2009), § 42.

285 *Ibid*., § 43.

Such activities in public space are to be distinguished from private activities in public, which the person carries out purely or primarily for personal fulfilment[286] as well as those activities in public, in which the person cannot be said to be participating voluntarily. An example of the latter may be found in activities in which a person is particularly vulnerable. As the Court noted in Peck v. UK, while the applicant was in a public street 'he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night, he was deeply perturbed and in a state of some distress'.[287] Not only was Peck not involved in any particular social activity with others, he might not have had actual choice not to go into public space due to his severe distress, which made him attempt to commit suicide.[288]

In von Hannover v. Germany, the Court confirmed that 'activities of a purely private nature' can take place in public and semi-public space (such as private beach clubs), where one is fully or partially exposed to the public view.[289] However, these private activities are understood in a very broad manner, encompassing daily life activities that happen to be carried out in public, including those of a mundane nature (Fennwick, 2017, p. 736). This means that large parts of our lives that we live out in public space, which are not essentially public in nature, such as having a walk with one's family, doing grocery shopping and jogging, are generally seen as private activities occurring in public space by the ECtHR.

Nevertheless, distinguishing between (essentially) private or public activity is very difficult, especially when it does not involve clear-cut textbook examples. The two objectives often mix in our activities – public activities can include important elements of the personal (or private) and personal elements can include elements of the public. Moreover, in both types of activities people participate also in order to establish and develop relationships with others (although to differing degrees). The Court confirmed this in Amann v. Switzerland, stating that there is no reason of principle to justify excluding activities of a professional or business nature form the notion of 'private life'.[290] Certainly, the Court should not interpret this distinction between private and public activities in a too strict and exclusionary manner, as that might lead to a

286 *Ibid*., § 42.

287 *Peck v. UK* (2003), § 62.

288 In related manner, Germany introduced an additional offense in 2014, covering the unlawful creation or transmission of 'pictures that showcase another person's helplessness, and thereby violat[e] their intimate privacy' (German CC § 201a(1)(2)); see Koops et al. (2018).

289 *von Hannover v. Germany* (2004).

290 *Amann v. Switzerland* (2000) Application no. 27798/95, § 65.

narrow protection solely of a person's 'inner life', going against a broad conception of Article 8 – a key interpretative principle of the Convention connected to the doctrine of effectiveness (Rainey et al., 2017, p. 76).

Furthermore, the Court seems to overlook the value of the right to respect for private life in relation to participation in (essentially) public activities, both those relating to informal civic activities (such as, sociability in public space) as well as formal civic activities (such as peaceful assembly and protesting) (Aston, 2017; also see Chapter 5).[291] That privacy is important for the democratic political system is an increasingly common claim in contemporary privacy scholarship (see Chapter 4). There is thus a strong connection between freedom of expression (Article 10 ECHR), freedom of assembly and association (Article 11; often read together with Article 10 by the Court) and the right to respect for private life (Article 8). Usually, the relationship between these rights (particularly between freedom of expression and right to respect for private life; see Rainey et al., 2017, pp. 503–505) is portrayed as in conflict (which sometimes it is, most often in relation to publication of personal information in the media).[292] However, I am here referring to their relationship that serves the same function and amounts to somewhat of an overlap. As Goold (2010, pp. 42–43) put it, it is difficult to imagine 'being able to enjoy freedom of expression, freedom of association or freedom of religion without some accompanying right of privacy.'

All of the mentioned rights are necessary for the constitution and functioning of a democratic society, although they go about ensuring this in different ways. Freedom of expression protects the expression of all types of ideas, including those that 'offend, shock or disturb the State or any sector of the population'.[293] Freedom of association protects peaceful assembly (including peaceful protest, especially when read together with Article 10) and the right to choose whether or not to form and join associations such as political parties, trade unions, and also other organisations, such as lodges of Freemasons (Rainey et al., 2017, p. 527). And privacy (in general, rather than referring to the right to respect for private life in Article 8 specifically), in this context, protects the possibility of participating in informal and formal civic activities,

291 As I have already mentioned in Chapter 3 (Section 4.2.4), I understand the right to respect for private life as referring to the human right to respect for 'privacy'. That is, the use the term 'private life' seems to be related to the important role of the French language in drafting the Convention (private life being a somewhat awkward rendering of 'vie privée'), rather than having any legal or particular theoretical consequences (see Schabas, 2017, p. 369).

292 E.g. *von Hannover v. Germany* (2004); *Axel Springer AG v. Germany* (2012) Application no. 39954/08.

293 *Handyside v. UK* (1976) Application no. 5493/72, § 48.

thorough preserving possibilities of being obscure and inconspicuous in public space and fostering the possibilities of formation of different types of social relations as well as the formation and representation of different publics (see Chapters 4 and 5).[294]

As the Court stated in relation to the freedom of expression, without 'pluralism, tolerance and broadmindedness' there is no democratic society.[295] In order for such pluralism to emerge, however, more than the protection of expression and (political) association is needed (cf. Hughes, 2012, p. 230). What is needed is the protection of possibilities ('breathing space') that allow people to develop themselves into political beings (development of political autonomy). This not only requires the possibility to retire to a private space ('a room of one's own') but also the possibility to be present and active (including a level of civil disobedience) in common public space with like-minded and different-minded people without constant scrutiny, influence of behaviour (such as nudging), and possible detrimental consequences in the future (e.g. getting fired or put on a list of potential troublemakers based on association with a certain group or person).[296] In the context of public life – participating in public space and in public activities, such as demonstrations or celebrations – one develops one's social identity. She does this not by developing the closest ties with others but by developing a sense of communal life, by forming more or less loose ties with those alike and those different. In this way, democratic values such as pluralism, tolerance and broadmindedness are also developed. In order to recognise and protect this societal value of privacy, the Court could extend its newly coined notion of 'the right to lead a private social life' from the workplace to multi-purpose public space and, ideally, recognise its connection to political activity. Of course, such a right would

294 While a large part of the power of political participation is indeed based on being seen (a large mass of protesters has a greater political impact than a handful), this visibility relates to a particular type of visibility while still preserving anonymity (see Chapter 4).

295 *Handyside v. UK* (1976) Application no. 5493/72, § 48.

296 Such an interpretation is confirmed with empirical data based on interviews with persons being subject to overt police surveillance at political meetings, demonstration rallies and other forms of protest. This data suggests that such surveillance was perceived as being (1) physically and psychologically intrusive, (2) restricting social and political interaction and (3) reducing [political] autonomy (Aston, 2017). Impacts of surveillance on associations include impact on fundraising, relations with members, reputation and connection with allies, redirection of agendas, displacement of strategic framing, and foreclosure of space for civil disobedience (Starr, Fernandez, Amster, Wood, & Caro, 2008). Starr et al. (2008, p. 267) found that instead of leading to the customary dualism in which hardcore activists become more militant, while others become more moderate, they found signs of pervasive pacification – organisations were found to be abandoning 'grey area' civil disobedience activities and moving toward doing exclusively educational and permitted activities. However, even in this context, surveillance has led to reduction and self-censorship.

not be unlimited and the Article 8(2) test would need to be performed. What such recognition might achieve, however, is a slight tilting of the balancing act between privacy and other societal interests (such as prevention of disorder) in favour of privacy, now seen as a societal interest as well. Indeed, in FNASS and Others v. France v. France, the Court has already stated that the right to lead a private social life 'may include professional activities or *activities taking place in a public context*',[297] potentially broadening the scope of this right from the workplace to open public spaces as well.

I do not mean to suggest, however, that Article 8 should protect every public activity a person might seek to engage in with other human beings in order to establish and develop such relationships or to participate in political activity. Indeed, as the Court stated in Friend and the Countryside Alliance and others v. UK, concerning fox hunting, a broad construction of Article 8 does not mean that it protects every activity a person might seek to engage in with other human beings in order to establish and develop such a relationship.[298] Notably, it does not protect 'interpersonal relations of such broad and indeterminate scope that there can be no conceivable direct link between the action or inaction of a State and a person's private life'.[299] What exactly this 'direct link' means is, intentionally, left to interpretation and application to concrete circumstances of the case at hand.

However, as the Court noted itself in relation to Article 11 (freedom of assembly and association), pluralism is built upon recognition of the 'diversity and the dynamics of cultural traditions, ethnic and cultural identities, religious beliefs, artistic, literary and socio-economic ideas and concepts'.[300] Yet, pluralistic interaction does not occur only or even primarily within organisations (whatever their purpose), it mostly occurs through mere presence and everyday activity in public space, thus possibly not engaging Article 11. Measures interfering with these possibilities (more concrete examples of which are found in Chapter 5) might amount to a subtler or lesser

297 *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France* (2018), § 153; emphasis added.

298 *Friend and the Countryside Alliance and others v. UK* (2009), § 41.

299 *Botta v. Italy* (1998) Application no. 21439/93, § 35.

300 *Gorzelik and others v. Poland* (2004) Application no. 44158/98, § 92.

interference than those recognised in relation to either Article 10 or 11 ECHR.[301] While the Court has held that different types of measures (ranging from prohibitions to restrictions) affecting Articles 10 and 11 that might lead to a chilling effect, can amount to an interference,[302] protection – especially in relation to access, participation and surveillance in public space – might be strengthened, if Article 8 would be considered as well. Nevertheless, the Court has been very reserved in recognising the role of privacy for society (beyond its role for the individual) and for preserving democracy.[303] As such, this area is underdeveloped (Hughes, 2012, p. 227). This connection between the three rights is particularly interesting and is in need of further examination, going beyond the scope of this dissertation.

Besides the nature of the activity taking place in public space, the Court seems to attach even more importance to the question, whether data relating to a person's private life were created, stored and have been further used or disseminated. In view of the proliferating use of digital technology in public space, this third key factor will therefore be the most relevant for determining the scope of protection of private life in public space.

5. BEYOND 'PRIVATE' DATA: DATA FROM THE PUBLIC DOMAIN

The ECtHR has emphasised that the broadly constructed right to respect for private life, which includes the right to establish and develop relationships with others, corresponds – at least in general – with the 1981 Convention for the protection of individuals with regard to automatic processing of personal data of the Council

301 For example, in *Pálomo Sanchez and others v. Spain* (2011) Applications nos. 28955/06, 28957/06, 28959/06 and 28964/06, no violation of Article 10 was found where the applicants claimed dismissal from their jobs due to trade union activities. In *Appleby and others v. UK* (2003), Application no. 44306/98, the Court found that there was no violation of Article 10 where the applicant argued that the State should guarantee access to a public space on a privately-owned shopping mall.

302 In regard to revealing journalistic sources (Article 10): Roemen and Schmit v. Luxembourg (2003), Ressiot and others v. France (2012), Nagla v. Latvia (2013), Goodwin v. UK (App. 17488/90, 1996), Keena and Kennedy v. Ireland (2014). Concerning Article 11 (disallowing or ending protests) see, e.g., Baczkowski and others v. Poland (2007); Patyi and others v. Hungary (2008).

303 It has recognised it in a few cases, e.g. *Klass and Others v. Germany* (1978) Application no. 5029/71, § 48-9); *Malone v. UK* (1984) Application no. 8691/79, §81; *Kennedy v. UK* (2010) Application no. 26839/05, § 167 (as referred to in Hughes, 2012, p. 234).

of Europe (1981 CoE Convention).[304] Particularly since the mid-1980s the Court increasingly uses insights and principles from data protection regulation to consider issues raised by modern technologies (De Hert & Gutwirth, 2009, p. 18). According to the Court, the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention.[305] The Court has thus associated its broad interpretation of the notion of 'private life' in Article 8 with the notion of 'personal data' from data protection laws.

However, while the Court has referred to the term 'personal data' several times, in particular using the definition from the 1981 CoE Convention,[306] it usually avoids its use and instead uses the expression 'data [or information] relating to private life'.[307] While the terms 'personal data' and 'data relating to private life' overlap to a significant extent,[308] it should be noted that not all personal data falls within the scope of protection granted by Article 8(1). This means that processing of personal data will only fall within the scope of Article 8, *if* it affects the private life of individuals. For instance, in the case of Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium, the Court did not find an interference with private life, as no data from the video monitoring of public space was stored and thus could not be subsequently used (the specific factors used by the Court to assess this distinction will be examined later in this section, after relevant case law is reviewed).

Particularly relevant for the purpose of this Chapter is the fact that the Court in several cases acknowledged that also the data about persons in the public domain may fall within the scope of Article 8, at least once they are systematically stored.[309] For

304 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty no. 108), 28.01.191; the purpose of this Convention is 'to secure … for every individual … respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him' (Article 1), which the Court confirmed in its judgments (e.g. Rotaru v. Romania (2000), § 43).

305 *Z v. Finland* (1997) Application no. 22009/93, § 95.

306 Article 2 1981 CoE defines personal data as 'any information relating to an identified or identifiable individual'. See judgments: *Amann v. Switzerland* (2000), § 65-67; P.G. and J.H. v. UK (2001), § 57.

307 E.g. *Copland v. the United Kingdom* (2007) Application no. 62617/00, § 43.

308 For a more detailed review of the relationship between the two notions, see De Hert & Gutwirth (2009) (2009).

309 *Amann v. Switzerland* (2000), § 65; *Rotaru v. Romania* (2000), § 43–44; *P.G. and J.H.* (2001), § 57–58; *Segerstedt-Wiberg and others v. Sweden* (2009) Application No. 62332/00, § 72; *Leander v. Sweden* (1987) Application no. 9248/81, § 48.

instance, in Amann v. Switzerland, a case concerning a file on an individual held by intelligence services, stating that the person was in contact with the Russian embassy, the Court confirmed that the storing of data relating to 'private life' of an individual does indeed fall within Article 8(1).[310] In this case, the Court famously declared that

> 'it is not for the Court to speculate as to whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way. It is sufficient for it to find that *data relating to the private life of an individual* were stored by a public authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference'.[311]

This echoes a much earlier decision from 1984 in Malone v. UK, in which the Court considered that the mere possibility of a transfer of 'metering records', which register the numbers dialled on a particular telephone and the time and duration of the call, can give rise to issues under Article 8, 'quite apart from any concrete measure of implementation taken against the applicant'.[312]

However, earlier ECtHR case law did not always follow this logic. In the case of Friedl v. Austria, where photographs were taken of the applicant at a public demonstration in a public place and retained by the police in a file, the Commission did not find an interference with private life, 'giving weight to the fact that the photograph was taken and retained as a record of the demonstration and no action had been taken to identify the persons photographed on that occasion by means of data processing'.[313] It seems that at the time there was a requirement of individual identifiability based on a factual, case-specific assessment, in order for the data to relate to private life. In later case law, especially after Amann v. Switzerland and Rotaru v. Romania, permanent or systematic recording and subsequent use of data – even if only potential – have become key factors (although not the only ones) for determining whether the data relates to an individual's private life. Nevertheless, based on this case law the data must still relate to an identified individual. One can thus broadly distinguish between an ECtHR and a data protection identifiability approach here. On the one hand, data protection law is very much hypothetical and future- or risk-oriented (see e.g. Gellert, 2020 forthcoming), thus requiring neither direct individual identifiability nor concrete harm. The ECtHR, on the other hand, while also not requiring concrete harm (at least as long systematic recording

310 *Amman v. Switzerland* (2000), § 65.

311 *Ibid.*, § 70; emphasis added.

312 *Malone v. UK* (1984), § 86.

313 *Friedl v. Austria* (1992), § 51-52; also *P.G. and J.H. v. UK* (2001), § 58.

of data takes place and the data relates to private life), does seem to require that data relate to an identified individual (assessed case by case by the Court) for private life to become involved. This has important consequences for contemporary surveillance of public space, which increasingly surveils persons as a part of a group (particularly an algorithmic group) rather than as particular individuals.

This might change in view of *in abstracto* complaints by 'potential victims', which the Court allows in certain specific situations. The Court accepts such complaints in cases, for example, where a person is not able to establish that the legislation he complained of had actually been applied to him on account of the secret nature of authorised measures,[314] or where a person is covered by the scope of legislation permitting secret surveillance measures and if the applicant has no remedies to challenge such covert surveillance.[315] Nevertheless, the applicant must produce *reasonable and convincing evidence of the likelihood that a violation affecting her personally* will occur; mere suspicion of conjecture is insufficient.[316] It is uncertain, whether this route might be successful when lodging a complaint to the Court and claiming that one is a 'potential victim' of the (more or less) overt surveillance apparatus of a particular smart city/living lab initiative. The argumentation here might be that because the (in principle overt) surveillance targets undisclosed algorithmic groups to which one might or might not fall in (depending on the parameters), the person is unable to offer proof or to substantiate that she is a victim of a violation. Considering the Court's living instrument approach of interpreting the Convention, particularly in relation to technological change, this kind of interpretation would be possible.

Data from the public domain' (sometimes referred to as 'public data') can therefore fall within the scope of private life where they are systematically collected and stored in files held by authorities.[317] Just as with the notion of 'public space', the Court does not define how it understands 'public data' but it is clear from its case law that it includes data that is in one way or another publicly available. In the Rotaru v. Romania case, for example, it declared that publicly available information about the applicant's life, in particular his studies, his political activities and his criminal record, which was systematically collected and stored in a file by the state, does fall within the scope of private life protected in Article 8(1).[318] The case concerned false and defamatory

314 *Klass and others v. Germany* (1978).

315 *Roman Zakharov v. Russia* (2015).

316 *Senator Lines GmBH v. fifteen member States of the European Union* (2004); emphasis added.

317 *Amann v. Switzerland* (2000), § 65; *Rotaru v. Romania* (2000), § 43.

318 *Rotaru v. Romania* (2000), § 44.

personal data in a file on an individual by the Romanian secret services, in particular that the applicant was a member of a legionnaire movement, which was an extreme right-wing, nationalist, anti-Semitic and paramilitary movement. In this case, which concerned very old, false and defamatory data, the Court declared that the mere storing of information relating to an individual's private life, just like the mere use or refusal to allow the applicant an opportunity to refute it, amounts to an interference with Article 8(1).[319]

Data that can be captured based on observation and recording of a person's appearance and verbal expression also fall under the rubric of publicly available data. In the P.G. and J.H. v. UK case, the Court decided that the recording of person's voices at the police station (whilst being charged with a crime in their cells), amounted to an interference with Article 8 because a permanent record had been made of the person's voice, which was then subject to a process of analysis directly relevant to identifying that person in the context of other personal data.[320] Somewhat similarly, the Court stated in Perry v. UK, the video camera 'ploy' case, that what is essential is the fact that the 'ploy' by the police went beyond the normal or expected use of a usual type of camera in the police station and that there was permanent recording of the footage and subsequent use, which amounted to processing or collecting personal data about the applicant.[321] In these cases, the Court thus recognised the right of individuals to have control, at least to a certain extent, of the use and registration of their personal data, and it acknowledged the basic idea behind one of the fundamental principles of data protection, namely, purpose limitation (in the sense that personal data cannot be used beyond normally foreseeable use; De Hert & Gutwirth, 2009, p. 19).

Data that is captured from public space via the use of surveillance technologies (even without the use of covert surveillance methods) can also fall under the Court's notion of 'data from the public domain'. The Court held in Uzun v. Germany, a case about covert GPS tracking of a car by the police, that the systematic collection and storing of data of a person's whereabouts and movements of a person in public space and further processed in order to draw up a pattern of his movement, can also lead to an interference with Article 8(1).[322] In a similar case, Shimovolos v. Russia, personal data was collected by the police, in particular data about journeys throughout the country

319 *Ibid*., § 46; also *Leander v. Sweden* (1987), § 48.

320 *P.G. and J.H. v. UK* (2001), § 59-60.

321 *Perry v. UK* (2003), § 41.

322 *Uzun v. Germany* (2010), § 51-52.

made by the applicant.[323] The applicant was registered in a so-called 'Surveillance Database' as a 'Human Rights Activist' amongst persons allegedly involved in extremist activities. Whenever a person in the database purchased a train or plane ticket, a state authority would receive an automatic notification. In this case, the Court confirmed that the systematic collection and storing of data by security services on particular individuals constituted an interference with these person's private lives, 'even if that data was collected in a public place' or 'concerned exclusively the person's professional or public activities'.[324] However, the Court did not offer any substantive arguments why the collection of such data constitutes an interference (for example, stating that it reflects personal choices and can lead to the identification of many other far more personal details, including one's place of work and home, one's favourite restaurant or one's lover).

In the case of Vukota-Bojić v. Switzerland, the applicant was systematically and intentionally watched and filmed in public spaces by professionals acting on the instructions of an insurance company.[325] The material that was obtained in public space did not relate to any particularly intimate activities, it was stored and selected for the purpose of using the captured images as a basis for an expert opinion and, ultimately, for a reassessment of the applicant's insurance benefits. The Court confirmed that due to the permanent nature of the footage and its further use in an insurance dispute may be regarded as processing or collecting of personal data about the applicant constituting an interference with Article 8(1).

In regard to data that is the result of video recording in the law-enforcement context, which can also be considered a type of data in the public domain, the Court has held on various occasions that the release of the applicant's photographs by police authorities to the media amounts to an interference with their right to respect for private life.[326] In this latter type of case law, it is possible to claim that one should reasonably foresee that law enforcement will take certain steps in order to capture and record data in the name of public interest. In Khmel v. Russia, the Russian government thus stated 'that a person who had committed offences or crimes should envisage various restrictions on his or her rights, including the right to respect for private life. After the applicant had committed a breach of public order, caused damage to the honour and dignity

323 *Shimovolos v. Russia* (2011).

324 *Ibid*., § 65; also *Amann v. Switzerland* (2000), § 65-67; *Rotaru v. Romania* (2000), § 43-44.

325 *Vukota-Bojić v. Switzerland* (2016), § 58.

326 *Khmel v. Russia* (2013), § 41; Sciacca v. Italy (2005); *Khuzhin and Others v. Russia* (2009) Application no. 13470/02.

of the authorities and been escorted to the police station, his private life had been brought into the public domain.' While the Court in the above referred cases did not state this explicitly, it might be argued that in such cases, the interference occurs only or primarily when the data is distributed to the media and then published.

Following De Hert and Gutwirth (2009, p. 26), the four relevant factors that are used by the ECtHR in order to distinguish between data that relate to one's private life and those that do not can be summed up as such: (1) whether the data are considered to be closely linked to the private sphere of individuals – whether the data is 'private'; (2) whether there is systematic storage of data; (3) whether the data relate to an identifiable individual; and (4) whether the data subject could reasonably expect the subsequent use or other processing. From these criteria and the above examined case law it is clear that public activities, at least those that cannot be called 'essentially public activities', can also fall within the scope of Article 8, when the creation of data is involved through the use of technology that allows for the collection and storage, particularly systematic, and subsequent analysis and use of thusly gathered data.

This means that there can be an interference with Article 8(1) even when the data involved is not particularly sensitive, for example, capturing a person's movements in the centre of one's hometown, walking down the street and entering a store to do grocery shopping. This is important especially in view of present-day cases of surveillance of public space, where such 'insensitive' data is so often captured, stored and analysed. What is important to note here is the fact that such data can through contemporary types of processing and aggregation techniques lead to all sorts of inferred data, thus subsequently revealing far more private and sensitive data about an individual. The rapid development of technology is often acknowledged in Article 8 case law, as it was in the Shimovolos v. Russia case, where the Court noted in its assessment of the requirements of Article 8(2) that it is essential to have clear and detailed rules on the application of secret measures of surveillance, 'especially as the technology available for use is continually becoming more sophisticated'.[327]

Finding an interference with a person's private life, however, does not suffice to find a breach of Article 8; the interference must also be found illegitimate. In the following sections I will therefore examine how stringent or lax are the requirements for an intrusion into one's private life when done by the state and in relation to the state's positive obligations, when the intrusion is done by private actors.

327 *Shimovolos v. Russia* (2011), § 86.

6. REQUIREMENTS FOR A LEGITIMATE INTERFERENCE INTO ONE'S PRIVATE LIFE IN PUBLIC

6.1 Article 8(2) assessment: interference by the state

The above examination of ECtHR case law shows that the scope of Article 8 indeed includes protection of private life in public space. The right to respect for private life, however, is not inviolable – interference with this right is possible and is regulated in Article 8(2) ECHR. In fact, it is often claimed that private life in public, if at all, deserves only very weak protection, as the intrusion into privacy is only minor (for a discussion and rejection of this argument, see Nissenbaum, 1998, 2010). Indeed, the Court itself seems to sometimes share this view. Such was the case in the Uzun v. Germany case, where the applicant's location and movements in public space were tracked via GPS. While determining the requirements for interference with the right to private life in these circumstances, the Court held that the standards guaranteeing protection against abuse need not be as strict as those established in the context of surveillance of communications, which is considered one of the most intrusive surveillance measures, since 'surveillance via GPS of movements in public spaces and thus a measure, which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations'.[328] The Court posited:

> 'GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings'.[329]

Nevertheless, even in cases of such lesser (or less deep) intrusion into the right to respect for private life, the Court consistently sets a range of requirements for the intrusion to be justified.

In previous sections, I have considered wide-ranging types of intrusions together. However, these need to be distinguished to a higher degree in regard to Article 8(2) assessment, as the types of specific requirements the Court imposes on them is very much based on the type of intrusion and the specific context of the case. For the purposes of this Chapter, where my main concern is to show the existence and the

328 *Uzun v. Germany* (2010), § 66.

329 *Ibid*., § 52.

scope of the right to respect for private life in public, I will examine the requirements for the state's interference in one's private life by focusing on the most notable cases in this context.

The Court has developed a flexible methodology for the interpretation and application of paragraph 2 in determining whether the interference with the right is actually in breach of the Convention (Schabas, 2017, p. 402). The first step of the Article 8(2) assessment, is to determine whether the interference is in accordance with the law, referring to the broad, general notion of the 'rule of law'. There needs to be some basis in the domestic law (formal requirement), which needs to be accessible to the individual and its consequences for the person must also be foreseeable (substantive requirement).[330] Most cases before the Court are examined only in regard to the first step, as the Court does not consider it necessary to examine either the second (legitimate aim) or the third step (necessary in a democratic society) (*ibid*., p. 403-6), if it finds that the first step was not satisfied. In fact, the legitimate purpose requirement is 'rarely very significant, given the breadth of what is permissible under article 8' (*ibid*., p. 404), so I will not discuss it further. Instead I will focus on the first and third step of the Court's assessment.

Even in the context of national security, the law must be sufficiently clear so as to give citizens an adequate indication concerning the circumstances in which and the conditions on which the public authorities are empowered to resort to secret surveillance. In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.[331] As I am mostly interested in intrusions that fall outside of the scope of national security, dealing with the prevention of crime and disorder (arguably the most commonly used legitimate purpose), the requirement of foreseeability will be strict.

In Vukota-Bojić v. Switzerland, a case of monitoring an individual in public space for the purpose of detecting insurance fraud, the Court found a violation of Article 8 because domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on insurance companies acting as public

330 E.g. *Malone v. UK* (1984), § 66; *Leander v. Sweden* (1987), § 50.

331 *Leander v. Sweden* (1987), § 51; *Malone v. UK* (1984), § 68.

authorities conducting secret surveillance of insured persons.[332] Furthermore, echoing the above remarks concerning GPS surveillance made in Uzun v. Germany, the Court noted that the surveillance in the present case – taking place in public space – must be considered to interfere less with a person's private life than, for instance, telephone tapping, thus amounting to an arguably minor interference with the applicant's Article 8 rights.[333] In this, the Court is referring to the claim made by the German Federal Court (*Bundesgerichtshof*) in a leading judgment on the matter of secret surveillance of an insured person ordered by an insurer (8C_807/2008, 15 June 2009). In this case the German court held that regular surveillance of insured persons by private detectives represents a relatively minor interference with the fundamental rights of the individual concerned. This is in particular so because the aim of such surveillance is 'to collect and confirm facts which materialise in the public domain and may be observed by anyone (for example, walking, climbing stairs, driving, carrying loads or performing sports activities)'.[334] Importantly, by noting this in its judgment the ECtHR confirmed that even activities in which the interference with one's private life is relatively minor must nevertheless adhere to the general principles on adequate protection against arbitrary interference with Article 8.[335]

In Uzun v. Germany, on the contrary, the Court concluded that the secret surveillance measures were 'in accordance with the law'. Not only did the Court determine that the law was clear and foreseeable enough, it also examined whether there had been adequate and effective guarantees against abuse, since possibilities of arbitrary interference in secret surveillance are particularly high.[336] The Court based this assessment on several criteria: (1) the nature, scope and duration of the measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out and supervise them; and (4) the kind of remedy provided by national law.[337] Since the GPS surveillance was considered to interfere less with a person's private life, the

332 *Vukota-Bojić v. Switzerland* (2016) § 74-7.

333 *Ibid*., § 76-7.

334 As quoted in *Vukota-Bojić v. Switzerland* (2016), § 43.

335 *Ibid*., § 76.

336 *Uzun v. Germany* (2010), § 63.

337 *Ibid*., § 63; also *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (2007) Application no. 62540/00, § 77

Court did not apply the strictest requirements for communications surveillance.[338] Instead, it applied the above 'general principles on adequate protection against arbitrary interference with Article 8'.[339] The Court found that even though there was no fixed statutory limit on the duration of GPS monitoring, the duration was subjected to a proportionality test by national courts and there was the possibility to exclude evidence from an illegal GPS surveillance in court.[340] Furthermore, the grounds for authorising this measure were quite strict, against a person suspected of a criminal offence of considerable gravity.[341]

However, even if a restriction on private life is in accordance with the law and serves one of the legitimate objectives, this restriction must still be in accordance with the third step of Article 8(2) ECHR.

The third and last step of the Article 8(2) assessment, is whether the interference is 'necessary in a democratic society'. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, to consider whether the authorities have struck 'a fair balance between the competing interests of the individual and of society as a whole' (Schabas, 2017, p. 406; referring to Keegan v. Ireland 1994, § 49). This step has been said to be 'the most subjective part of the application of paragraph 2' (*ibid*., p. 406), involving more or less subtle distinctions about the proportionality of measures by the state that restrict human rights.[342] Notably, there is an important relationship between 'necessity' and 'democratic society', of which the hallmarks are pluralism, tolerance and broadmindedness (*ibid*., p. 406; referring to Handyside v. UK (1976), § 49). However, it has been noted that in

338 The Court sets the highest standards of protection against abuse in cases communication surveillance (e.g. *Zakharov v. Russia* (2015) Application no. 47143/06, § 67; *Liberty and others v. UK* (2008) Application no. 58243/00, § 62; *Weber and Saravia v. Germany* (2006) Application no. 54934/00, § 95, acknowledging the risk that such systems of protection pose a danger of undermining or even destroying democracy on the ground of defending it (*Klass and Others v. Germany* (1978), § 49-50; *Leander v. Sweden* (1987), § 60).

339 *Uzun v. Germany* (2010), § 66.

340 *Ibid*., § 69 and 72.

341 *Ibid*., § 70.

342 The Court allows the state a certain 'margin of appreciation' in applying the 'necessary in a democratic society test', recognising that its role is not to sit as a tribunal of fourth instance and that it is also not as well positioned as the national legal institutions to assess many of the relevant factors (Schabas, 2017, p. 406). The Court has recognised the highest margin of appreciation in cases concerning morality, ethics and social policy and other cases where there is no or little consensus (*ibid*.).

the majority of cases, including those examined in this Chapter, the Court examined only the proportionality requirement (cf. De Hert & Gutwirth, 2009, p. 22).

The assessment of proportionality necessitates balancing the right of the individual against the interest of the state and the particular society. In particular, the Court takes into account the nature of the measure taken (including its reach, adverse consequences, the scope of abuse of the measure), whether there are other possible measures that are less intrusive or whether the state could have implemented the particular measure in a less drastic way, the status of persons involved (prisoners, public persons) and whether there are any safeguards that can compensate for the infringement of rights that a measure can create (*ibid*., pp. 22-23; referring to Delmas-Marty 1992, p. 71). In the Niemietz v. Germany case, for example, the Court found that the search of a lawyer's office, while pursuing a legitimate aim (prevention of crime and protecting the honour of a judge), was not proportionate to these aims. The warrant was drawn in broad terms (ordering a search for and seizure of 'documents' revealing the identity of the author of the offensive letter without any limitation), there was no independent observer present (not required under German law at the time) and the search seriously impinged on professional secrecy.[343] Furthermore, the attendant publicity was deemed capable of adversely affecting the applicant's professional reputation by the Court, in the eyes of both his existing clients and of the public at large.[344] As such, the Court found the measure was not necessary in a democratic society and that there was a breach of Article 8.

Another case in which the Court assessed whether the measure was 'necessary in a democratic society is Uzun v. Germany. Examining the proportionality of the measure, the Court noted that the authorities first employed measures that interfered less with the applicant's right to respect for private life (by installing transmitters into his car), however these were discovered and destroyed by the applicant. Thus, these methods were less intrusive but they were also less effective.[345] GPS surveillance was then added to a multitude of previously ordered and partly overlapping measures[346] by two state authorities, making the surveillance of the applicant's conduct 'quite

343 *Niemietz v. Germany* (1992), § 37.

344 *Ibid*., § 37.

345 *Uzun v. Germany* (2010), § 78.

346 The measures included video surveillance of the entry of the house where he lived, the interception of the telephones in that house and in a telephone-box situated nearby, and the interception of postal communications (Uzun v. Germany [2010], § 79).

extensive'.[347] Nevertheless, as the GPS surveillance was carried out for a relatively short period of time (three months), with some limitations on other ordered measures, the Court determined that this surveillance did not lead to 'total and comprehensive surveillance' (*ibid*., § 80; I discuss this standard in the following paragraph). Most importantly, the Court considered that given the severity of the crimes for which the applicant was suspected (several attempted murders of politicians and civil servants by bomb attacks) and the purpose of preventing further similar acts, the surveillance measure was proportionate to the legitimate aims pursued and thus necessary in a democratic society.

While the distinction between 'less intrusive' (like GPS tracking and the use of CCTV while in public space) and 'more intrusive surveillance measures' (like surveillance of communications) is intuitively attractive, it can be misleading. This is so in particular because of the commonly used aggregation of surveillance measures, as was also the case in Uzun v. Germany. Furthermore, these measures were carried out by two different state authorities, leading to a more serious interference with the applicant's private life, as the Court itself noted. While a measure such as GPS tracking *in itself* might indeed be less intrusive, its combination with other measures can lead to a rather detailed image of a person's private life, thus amounting to a more severe intrusion with Article 8. The Court partially took this issue into account in the Uzun case when performing the proportionality test, noting that relevant safeguards need to be in place in order to prevent a person's 'total surveillance' (*totale Überwachung*; a term used in German Federal Constitutional Court doctrine), which leads to a comprehensive picture of one's life. However, in German law this is a very high standard, which is very difficult to reach and is, because of this, almost never employed in practice in case law. The standard was not reached in Uzun v. Germany, which concerned less intrusive combinations of measures, which are much more common in practice. Nevertheless, the ECtHR did state that sufficient safeguards against abuse also require, in particular, that 'uncoordinated investigation measures taken by different authorities must be prevented and that, therefore, the prosecution, prior to ordering a suspect's surveillance via GPS, had to make sure that it was aware of further surveillance measures already in place'.[348] It was, however, satisfied that the German Federal Constitutional Court's doctrine on 'total surveillance' and the principle of proportionality amount to sufficient measure to prevent abuse.[349]

347 *Ibid*., § 80.

348 *Ibid*., § 73.

349 *Ibid*.

Nowadays, surveillance of public space is being primarily led by private actors, that is businesses (often in some sort of cooperation with public actors), so that the test examining the state's positive obligations is of particular importance here. In fact, many cases that I have examined in this Chapter were concerned with the issue of state's positive obligations under Article 8. I will examine this next.

6.2 Curtailing the actions of private actors: the state's positive obligations

It has come to be fully accepted that the object of Article 8 is essentially that of protecting the individual against arbitrary interference by public authorities.[350] Nevertheless, with the evolutive interpretation of the Convention the Court has developed the doctrine of the state's positive obligations. This doctrine states that Article 8 does not merely compel the state to abstain from interference with individuals' right to respect for private life but also includes various positive obligations that are inherent in an effective respect for private or family life.[351]

Arguably, the state's positive obligations have a growing importance in the jurisdiction of the ECtHR (Klatt, 2011, p. 691; Mowbray, 2004, p. 229). Indeed, as mentioned, numerous cases examined in this Chapter involved the issue of states' positive obligations in relation to interferences with the right to respect for private life done by private actors. The common justification for the judicial recognition of positive obligations under the ECHR is the claim that they aim to ensure that rights are practical and effective (Mowbray, 2004, p. 221). Notably, the Court has often remarked that it does not really matter whether it analyses a case in terms of a positive or a negative obligation, since in both cases a fair balance between the competing interests needs to be struck, so that the boundary between the two tests does not lend itself to precise definition.[352] In both contexts, regard must be had to the fair balance that needs to be struck between the competing interests of the individual and of the community as a whole. While these claims are open to debate,[353] this issue goes beyond the topic of

350 This was not always so. Jacques Velu (1973, pp. 20–21) wrote in the 1970s that the question of the persons on whom Article 8 imposes duties has been split between two schools: the first, which thinks that most of the provisions (including Article 8) bind both states and individuals, and the other, which thinks that it binds only states.

351 *von Hannover v. Germany* (2004), § 57; *López Ribalda and others v. Spain* (2018), § 60.

352 E.g. *Hatton and others v. UK* (2003) Application no. 36022/97, 2003, § 98.

353 For instance, Klatt (2011, p. 694) claims that the application of the proportionality test in detail is *fundamentally* different in both categories.

this Chapter. Instead, I will focus on the concrete proportionality tests that the Court performed in the key cases that I have examined in this Chapter.

As in regard to the state's negative obligations, states enjoy a certain margin of appreciation in regard to its positive obligations. States generally enjoy a wide range of possibilities concerning the means available to them in order to satisfy their positive obligations. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves.[354] In certain circumstances, the state's positive obligation will only be adequately complied with, if legislative provisions concerning relations between individuals provide a framework for reconciling the various interests, which compete for protection in the relevant context.[355] In particular, the Court has considered this necessary as effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake. It has decided that effective criminal-law provisions (including effective enforcement) was required, for example, in cases of serious sexual offences against minors,[356] an advertisement of sexual nature in the name of a minor on an internet dating site[357] and the respect of the physical integrity of hospital patients.[358] In other, less grave cases, for example concerning the protection of a person's image against abuse (as in von Hannover v. Germany and Reklos and Davourlis v. Greece), the Court noted that civil and other legal means are also appropriate safeguards to satisfy the state's positive obligations. In some cases, the Court is satisfied even if there is no legal framework, but courts have managed to strike a fair balance between the opposing rights in the case at hand (Köpke v. Germany).

The Court has initially been reserved in finding the state's positive obligations under Article 8 unfulfilled. In the 1998 case of Botta v. Italy, where access to the beach and the sea for handicapped people was sought (required by Italian law), the Court held that a state has positive obligations where there is a 'direct and immediate link between the measures sought by the applicant and the latter's private life'.[359] In this case, in which

354 *López Ribalda and others v. Spain* (2018), § 60; *von Hannover v. Germany* (2004), § 57; *Reklos v. Davourlis v. Greece* (2009), § 35; *Bărbulescu v. Romania* (2017), § 108.

355 *Bărbulescu v. Romania* (2017), § 115; *Köpke v. Germany* (2010), p. 10.

356 *X and Y v. the Netherlands* (1985) Application no. 8978/80; *M.C. v. Bulgaria* (2003) Application no. 39272/98.

357 *K.U. v. Finland* (2009) Application no. 2872/02.

358 *Codarcea v. Romania* (2009) Application no. 31675/04.

359 *Botta v. Italy* (1998), § 34.

the applicant claimed that he could not enjoy a normal social life that would enable him to participate in the life of the community because he did not have access to the sea, the Court did not find such a direct and immediate link.

However, in later Article 8 case law – at least regarding the right to respect for private life in public – it can be argued that the Court has increasingly found that states have not fulfilled their positive obligations in making the right to respect for private life effective.[360] In fact, the Court seems to employ a serious and rather strict approach to the positive obligations test, which seems to be *on par* with the Article 8(2) assessment (as can be seen from the examination below). Since the cases that concern an interference with the right to private life in public usually involve a less serious interference with a person's privacy, the Court's proportionality tests in such cases are of particular interest here.

In the case in Köpke v. Germany, a case of workplace surveillance in a supermarket, the Court examined whether a fair balance was struck in the context of the case between the applicant's right to respect for her private life and the employer's interest in protection of its property's rights.[361] The Court found that a prior substantiated suspicion of an offence – required by German case law at the time for video surveillance of the workplace – was proportionate to the aim of investigating the offence. Notably, the Court took the view that 'covert video surveillance at the workplace following substantiated suspicions of theft does not concern a person's private life to an extent which is comparable to the affection of essential aspects of private life by grave acts in respect of which the Court has considered protection by legislative provisions indispensable'.[362] In this case, the Court was satisfied that respect for private life could adequately be protected by domestic courts, which had developed important limits on such surveillance in its case law, without the state having been obliged to set up a legislative framework. Moreover, there were sufficient practical limitations to the surveillance at hand (the number of people seeing the video was very small, it was used only for the termination of the labour contract, it lasted only for two weeks), so that the interference with the applicant's private life was restricted to what was necessary in order to achieve the aims pursued. There had also not been any other equally effective means available to protect the employer's property rights. The Court thus decided that a fair balance, within the margin of

360 *Bărbulescu v. Romania* (2017); *Antović and Mirković v. Montenegro* (2018); *López Ribalda and others v. Spain* (2018); *Reklos and Davourlis v. Greece* (2009); *von Hannover v. Germany* (2004).

361 *Köpke v. Germany* (2000).

362 *Ibid*., p. 11.

appreciation, between the applicant's right to respect for her private life and the employer's interest in protecting its property rights had been struck. However, noting the threat of new technologies, the Court ended the judgment in a pensive way: 'The Court would observe, however, that the balance struck between the interests at issue by the domestic authorities does not appear to be the only possible way for them to comply with their obligations under the Convention. The competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies'.[363]

In a recent similar case about video surveillance at the workplace in a shop, the Court reached a different conclusion. In López Ribalda and others v. Spain, the Court again examined whether the state struck a fair balance between the applicants' right to respect for their private life and their employer's interest in the protection of its organisational and management rights concerning its property rights.[364] It distinguished the facts of this case with the ones in Köpke v. Germany, noting that in the present case the covert video surveillance did not follow a prior substantiated suspicion against the applicants and was consequently not aimed at any of them specifically, but rather indiscriminately on all of the staff working on the cash registers. Moreover, it lasted over weeks, without any time limit and during all working hours. The Court thus found that the decision to adopt surveillance measures was based on a general suspicion against all staff in view of irregularities which had previously been revealed by the shop manager.[365] Due to these reasons, the Court found that the employed measures were not proportional to the legitimate aim of protecting the employer's interest in the protection of its property rights.

In the context of workplace surveillance, there was another notable Court decision, although this one concerned communications surveillance rather than video surveillance. In Bărbulescu v. Romania, a case about extensive monitoring of communications at the workplace, the Court held that despite a lack of consensus on the matter between Member States, domestic authorities need to ensure that the introduction of measures by an employer to monitor correspondence and other communications, irrespective of the extent and duration of such measures, must be

363 *Ibid*., p. 13.

364 *López Ribalda and others v. Spain* (2018).

365 *Ibid*., § 68.

accompanied by adequate and sufficient safeguards against abuse.[366] This interpretation is likely connected to the fact that the Court considers communications surveillance as a more severe privacy intrusion (see discussion in Uzun v. Germany above), also leading to a very strict assessment of whether a fair balance has been struck.

In Bărbulescu, the Court offered an extensive number of factors to consider in order to determine whether a fair balance between the interests (employees' interests in respect for their private life and the employer's interest in ensuring the smooth running of the business) has been struck: (1) whether the employee has been notified about the monitoring, where the notification needs to be clear about the nature or the monitoring and given in advance; (2) the extent of the monitoring and the degree of intrusion into the employee's privacy (a distinction should be made between the monitoring of the flow and the content, whether all or only a part of the communication is monitored); (3) whether the employer has provided legitimate reasons to justify the monitoring and accessing their actual content; (4) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures (requiring an assessment based on particular circumstances); (5) the consequences of the monitoring for the employee and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure; (6) whether the employee had been provided with adequate safeguards (in particular, that the employer cannot access the actual content of the communications concerned unless the employee had been notified in advance of that eventuality); and (7) whether the employee has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful.[367] Notably, the Court held that the examination done by domestic courts of whether a fair balance has been struck, was done in a formal and theoretical manner, not examining all of the actual circumstances of the case and leaving several relevant questions identified above unanswered.[368] Consequently, the Court considered that domestic authorities did not afford adequate protection to the applicant's right to respect for his private life and correspondence (it considered these two together) and decided that there had been a violation of Article 8.

366 *Bărbulescu v. Romania* (2018), § 120; see also *Klass and others v. Germany* (1978), § 50; *Zakharov v. Russia* (2015), § 232-234. In the *Bărbulescu* case the Grand Chamber held a violation by eleven votes to six. The latter judges disagreed with the evaluation of the state's positive evaluations, preferring to grant a wide margin of appreciation to the state (§ 1, § 2 and § 5 of the Joint Dissenting Opinion).

367 *Bărbulescu v. Romania* (2017), § 121.

368 *Ibid*., § 139-140.

There are therefore many different ways of ensuring respect for private life, where the nature of the state's obligation will depend on the particular aspect of private life that is at issue and the concrete circumstances of the case at hand.[369] What can be observed from the above case law regarding positive obligations and the right to respect for private life in public is that the Court employs a rather strict proportionality test with numerous factors, even in cases where the intrusion into one's private life is, arguably, not very severe. While it does not, in such cases, necessarily impose the obligation to introduce a legal framework regulating a specific measure, it nevertheless often finds a violation of Article 8 based on a lack of implementation of other possible measures guaranteeing adequate protection of the right. This is of particular importance in regard to the increasing surveillance of public space conducted by private actors within smart cities and living labs, often taking place in a rather unregulated manner. In the concluding section I will refer to the main lessons of this analysis of ECtHR case law for privacy in public space and apply them to the example of the *Stratumseind Living Lab*, an illustrative example of surveillance of public space for purposes of security and monetary interests in a contemporary European city.

7. CONCLUSION: THE *STRATUMSEIND LIVING LAB* CONSIDERED THROUGH THE LENS OF ARTICLE 8

The above analysis of ECtHR case law has shown that the scope of protection of private life in public space is – perhaps somewhat surprisingly – rather broad. In fact, a subtle development in case law broadening the scope of private life so as to encompass diverse interferences with privacy in the public sphere can be discerned. This development is, of course, not linear. Nevertheless, the above analysis has resulted in several notable general developments of the right as well as in valuable specific insights that have particular value for privacy in public.

In order to analyse the scope of protection of private life in public, I have examined the Court's case law based on the three main categories that it employs: spaces, activities and data. In relation to the relevance of private space in the Court's assessment of the scope of private life a broader trend can be observed. While this factor played a relatively important role in older case law (as one of three factors),[370] it has almost completely disappeared from more recent Court's assessment. Quite the opposite,

369 E.g. *López Ribalda and others v. Spain* (2018), § 54; *Bărbulescu v. Romania* (2017), § 113; *Söderman v. Sweden* (2013) Application no. 5786/08, § 79.

370 *X v. UK* (1973); *Friedl v. Austria* (1994); *Lupker and others v. the Netherlands* (1992).

the Court now commonly stresses that the right to private life includes 'a zone of interaction with others even in a public context', so that intrusions into private life can also occur in physical public spaces.[371] On a more particular level, an interesting insight relating to public space can be discerned from the Gillan and Quinton v. UK judgment. In this judgment, the Court made a distinction between multiple- and designated-purpose types of space (particularly referring to streets and airports), where the latter might come with special surveillance needs that do not apply to public space in general (in the case of airports for purposes of security).[372] The Court concluded that distinct from designated-purpose types of spaces, one cannot really avoid open and multiple-purpose spaces, like streets. Following this line of thought, one could argue a bit further and conclude that the more multiple the purposes of use of the space at issue, the higher the reasonable expectation of privacy, as such space would potentially involve more parts of one's social life and one would not have a real (that is, acceptable) choice to avoid it. This might be a particularly valuable takeaway for considering the surveillance of multiple-purpose public space, as in cases of smart cities and living labs.

Concerning the types of activities that fall within the scope of private life, the above analysis showed that unlike with the type of place, this factor still plays an important role in ECtHR case law. In principle, only those activities that one carries out purely or primarily for personal fulfilment – which the Court calls 'private activities' – fall within the scope of private life. However, the Court understands this in a rather broad manner, so that this notion includes not only very private or intimate activities (e.g. having a romantic dinner with one's partner in a restaurant or kissing in a park) but also mundane activities of everyday life (e.g. grocery shopping and jogging). On the contrary, 'essentially public activities' do not fall within the scope of Article 8. The Court has referred to these as those activities, in which individuals *voluntarily expose* themselves to the public, so that they have little or no reasonable expectation of privacy.[373] The main idea here is that in relation to essentially public activities, amongst which the Court considered demonstrating and English fox hunting, the main reason for performing them is to be seen and heard. Based on such assessment, one might conclude that those activities in public, in which the person cannot be said to be participating voluntarily and which one does not do for personal fulfilment, for

371 E.g. *Peck v. the UK* (2003), § 57; *P.G. and J.H. v. UK* (2001), § 56; *Uzun v. Germany* (2010) Application No. 35623/05, § 43.

372 *Gillan and Quinton v. UK* (2010).

373 E.g. *Friend and the Countryside Alliance and others v. UK* (2009).

instance, because one is distressed (e.g. trying to commit suicide in public space, as in the case of Peck v. UK), also constitute private activities.

In relation to the distinction between private and public activities, another broader trend should be noted – the way the Court has been interpreting the right to respect for private life, where one of the main aims of this right is to develop one's personality. Already in the mid-1980s, the Court has established that one of the main purposes of Article 8 is to protect the right to establish and develop relationships with other persons, as these are necessary for the development of one's personality. With the Niemietz v. Germany judgment, the Court opened up the possibility of considering business and professional activities under this heading, positing that it is in the course of working lives that the majority of people have a significant opportunity of developing relationships with the outside world.[374] Recently, the Court seems to have gone a bit further, proclaiming that there is a 'right to lead a private *social life*', which serves the purpose of approaching others and developing one's social identity,[375] including not only professional activities but also other 'activities taking place in a public context'.[376] In the FNASS and others v. France case concerning anti-doping measures, athletes in the testing pool were required to provide a public authority with accurate, detailed and up-to-date information on their places of residence and their daily movements (both in private and public spaces; the 'whereabouts requirement'), seven days a week.[377] The Court saw this broad whereabouts requirement, which was also binding, as an interference with an individual's right to a private *social life* and an interference with personal autonomy.[378]

The Court has not yet properly developed the content and scope of private social life and 'activities taking place in a public context', which is not surprising since this is a very recent development (the Bărbulescu v. Romania judgment is from 2017). Nonetheless, one can carefully speculate that this development might be used in the future to recognise and protect increasing aspects of the societal value of privacy. As I have discussed in Chapter 3, people participate to develop their social identities, including their development into fully-developed citizen, both in private and public activities. Particularly in relation to activities connected to informal social life

374 *Niemietz v. Germany* (1992), § 29, Series A no. 251B.

375 *Bărbulescu v. Romania* (2017).

376 National Federation of Sportspersons' Associations and Unions [FNASS] and others v. France (2018).

377 National Federation of Sportspersons' Associations and Unions [FNASS] and others v. France (2018), § 156.

378 Ibid., § 151 and 153.

occurring in public places (especially multi-purpose ones), this seems to be a line of argument to be considered. A further line of reasoning might be to consider the role of privacy for democracy and political participation, that is, essentially public activities. The possibility for persons to develop themselves into political beings, to be present and active in public space without constant scrutiny, influence of behaviour and possible detrimental consequences in the future and other spheres of one's life, also merits protection. While this is already partially protected by Articles 10 (freedom of expression) and 11 (freedom of assembly and association), the role of Article 8 in furthering those goals has not yet been properly explored. The connection between the three rights is particularly interesting and is in need of further examination, unfortunately going beyond the scope of this dissertation.

Finally, I have examined the role of data (public or private) in regard to the scope of Article 8. Based on the above analysis of case law, the question whether 'data relating to private life' have been stored and/or analysed is arguably the most important factor in the Court's assessment, whether the interference falls within the scope of the right. For instance, in the case of video surveillance of public space without the recording of data, the Court has found no interference with Article 8.[379] When data is stored or the recording is systematic, the assessment changes and Article 8 applies.[380] The four relevant factors that are used by the ECtHR (alternatively rather than cumulatively) in order to distinguish between data that relate to one's private life and those that do not can be summed up as follows: (1) whether the data are considered to be closely linked to the private sphere of individuals – whether the data is 'private'; (2) whether there is systematic storage of data; (3) whether the data relate to an identifiable individual; or (4) whether the data subject could reasonably expect the subsequent use or other processing (cf. De Hert & Gutwirth, 2009, p. 26).

Notably, storing or systematically collecting 'non-private' data, such as data relating to one's public life (e.g. participation in a political party), can also amount to an interference with one's private life.[381] However, what is required is that the data relate to an identified individual (assessed case by case by the Court) for private life to become involved. In contrast to data protection law, the ECtHR seems to understand this criterion differently. Rather than a risk-based approach, where indirect identifiability suffices, the ECtHR seems to require a more factual, case-specific assessment. For example, in Friedl v. Austria, where photographs were taken and retained as a

379 *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium* (1998); Peck v. UK (2003).

380 E.g. *Vukota-Bojić v. Switzerland* (2016); *Uzun v. Germany* (2010).

381 E.g. *Rotaru v. Romania* (2000).

record of the demonstration, but no action had been taken to identify the persons photographed on that occasion by means of data processing, led the Court to conclude that Article 8 was not interfered with.[382] This might have important implications for contemporary types of surveillance, where persons are surveilled as a multiplicity (a part of a group, rather than individuals; see Chapter 5). While individuals are not directly identified (although they remain indirectly identifiable, in regard to future processing and data collection), they are nevertheless individually 'reachable' (Barocas & Nissenbaum, 2014, p. 45). In view of admissibility of *in abstracto* claims in certain cases, however, there seems to be a window of possibility for cases of interference with such group privacy as well.

In order to determine whether a person's private life has been interfered with in public, the Court established several (again, alternative rather than cumulative) factors in recent case law: (1) whether a person knowingly and intentionally involves herself in activities which are or may be recorded in a public manner; (2) a person's reasonable expectation of privacy; (3) whether a systematic or permanent record has been made of such material in the public domain; (4) whether there is a compilation of data on a particular individual; or (5) whether there has been processing or use of personal data, including the publication of the material concerned, in a manner or degree beyond that normally foreseeable.[383]

Considering the assessment of Article 8(2) as well as positive obligations of the state, one can conclude that even in the case of relatively minor interferences with the right to respect for private life (such as GPS-tracking of persons in public space), the general criteria against arbitrary interference need to be satisfied. These include: (1) the nature, scope and duration of the measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out and supervise them; and (4) the kind of remedy provided by national law.[384] The criteria concerning the state's positive obligations in recent case law concerning privacy in public have proven to be on par with those concerning the assessment of para. 2. In its assessment whether the state struck a fair balance between the applicants' right to respect for their private life and the competing right or interest (e.g. the employer's interest in the protection of its property rights), the Court examined several factors, particularly: whether the national legislative framework (or domestic courts) posed sufficient limitations

382 *Friedl v. Austria* (1994).

383 Based on: *Uzun v. Germany* (2010), § 44-45; *Perry v. UK* (2003), § 37-38; *P.G. and J.H. v. UK* (2001) § 57; *Peck v. UK* (2003) § 58-59; *Rotaru v. Romania* (2000) § 43-44; *Vukota-Bojić v. Switzerland* (2016) § 55-56.

384 *Uzun v. Germany* (2010), § 63.

to such surveillance; whether there was prior substantiated suspicion (rather than general suspicion) before surveillance was employed; whether surveillance was indiscriminate or aiming at a particular suspect; the length of surveillance measures; and whether the surveillance was clearly notified and in sufficient detail.[385] In the case of more intrusive surveillance, as in the case of communications monitoring (at the workplace), the Court set even higher standards that needed to be fulfilled.[386] Furthermore, the Court has made clear that a clear and detailed notification of surveillance (e.g. by an employer) cannot reduce the right to lead a private social life to zero. This is particularly important in the case of the *Stratumseind Living Lab* and similar initiatives, indicating that a notification of the types of surveillance on the street would not suffice to solve all privacy issues. The Court has also noted the characteristic of networked surveillance, according to which surveillance technologies and practices do not operate in isolation, in fact, they have a tendency to merge and spread. It thus stated that a combination of surveillance measures (even if in themselves minor interferences) can lead to a detailed image of a person's private life and, thus, potentially amount to a serious intrusion into one's private life.[387]

Based on this succinct analysis recap, I will thus briefly speculate over the Court's decision in relation to a complaint concerning the surveillance within the *Stratumseind Living Lab*.[388]

First, I need to examine, whether the surveillant practices taking place within the *SLL* could fall within the scope of Article 8. The Court would likely examine the case from the perspective of the general right to respect for private life. The mere fact that surveillance is occurring in public space does not hinder the applicability of Article 8. In this case, the public space involved is a street in the centre of the city – an open, multi-purpose public place. As such, people might not easily avoid it. Perhaps it is the closest way to one's home, perhaps persons work on the street and, moreover, it is a very popular nightlife destination, which someone might *need* to visit in order to socialise with friends and strangers that frequent it. As the Court suggested in Gillan and Quinton v. UK, people need to go about in multi-purpose public space without undue interference.[389] Also, due to the multi-purpose type of public space in question,

385 E.g. *López Ribalda and others v. Spain* (2018); *Köpke v. Germany* (2000).

386 *Bărbulescu v. Romania* (2017).

387 *Uzun v. Germany* (2010).

388 For the purposes of this hypothetical assessment, I am assuming that all of the national legal resources have been exhausted and the ECtHR would find the case admissible.

389 *Gillan and Quinton v. UK* (2010).

it would potentially involve more parts of one's private (social) life and one would not have a real (that is, acceptable) choice to avoid it. As such, it might feature a higher reasonable expectation of privacy than certain designated-purpose public spaces, such as airports. Consequently, the Court might consider the fact that surveillance is effected in such public space as an aggravating element of the possible interference.

Considering the type of activities regularly taking place on the Stratumseind street, one could consider them private activities. Stratumseind is a street with numerous pubs, where people go to drink and socialise with friends and strangers. In view of the right to lead a private social life, even in a public context, it is becoming clearer that socialising with lovers, friends and others in public space, plays an important part in developing one's individual and social identities. As I've argued in Chapter 5, the introduction of widespread and systematic surveillance that would monitor this aspect of persons' lives could have a serious detrimental effect on their autonomy and identity development and, as such, might represent an intrusion into one's private life. In regard to the reasonable expectation of privacy in this case (which is only one factor among others in the assessment), one should point out that persons would not expect such surveillance on the street. While they are probably aware of the CCTV in the city centre, they are likely not aware of the additional video and sound cameras with embedded capabilities, mood sensing and wifi tracking (especially in view of the absence of a sign on the street). However, as noted above, even a diligent notification of such surveillance would not fully mitigate this issue, as a person's right to private social life cannot be reduced to zero.

The Court would then examine, whether such surveillance of public space also records data, especially in a systematic manner, possibly leading to subsequent use in the future. This is, indeed, the case in the *SLL* (although it remains unknown to what extent exactly). However, there is an additional requirement in this regard – the data must relate to an individual. As pointed out above, the Court seems to require a factual, case-specific assessment in this regard. However, in the *SLL*, persons are mostly not actually individually identified (although this does not necessarily hold for the 'undesirables', who are to be tightly controlled or excluded from the street; in this case the standard is reached). This could be seen as the biggest potential limitation of Article 8 in regard to protecting privacy in public space, where people are nowadays commonly surveilled as a part of an algorithmic group. Nevertheless, given the evolutive approach to the interpretation of its rights, the Court might find that individual 'reachability' without individual identifiability suffices (e.g. with the use of *in abstracto* claims). One should also point out that the Court does not require concrete harm from the interference to emerge – risk of harm is enough. In practice, the Court

has not been shy in recognising rather abstract risks for identity-development. For these reasons, one could speculate that the Court would find the activities within the *SLL* as interfering with the right to respect for private life.

This conclusion would then be followed by an assessment, whether the interference was lawful or whether the state has struck a fair balance between the opposing interests in regard to its positive obligations. The aim of surveillance, in this case concerning both safety and protection of private property, would likely be considered legitimate, so I will not discuss it further.

It is unclear which type of assessment the Court would choose in the case of the *SLL*, organised in the form of a PPP, where the majority of the surveillance is performed by private actors on behalf of the municipality. This might depend on the assessment of actual power-relations within the PPP or would simply be dealt with by designating the municipality as the central actor in the PPP. In any case, as the Court pointed out itself, these two assessments do not essentially differ from each other, in fact, based on my examination above, they seem rather *on par*. Considering the type of surveillance on the Stratumseind street, one can conclude that it would be not seen as the most intrusive type of surveillance, such as communications monitoring. However, it might also not be seen as only a minor interference, as ordinary video monitoring of public space. The *SLL*, namely, consists of numerous, increasingly sophisticated digital technologies, which also aim to directly affect persons' behaviour. While in themselves they might not amount to a very serious interference, when taken together they might constitute a deeper intrusion. As such, I would argue that this might seem a rather serious intrusion in the view of the Court, despite its benevolent aim.[390]

The determination of the level of intrusion would then determine the level of safeguards that need to be in place, both legal and practical. In the case of an Article 8(2) assessment, the Court would examine whether the measures are in accordance with the law. In this case, it would establish that apart from a single general provision concerning video surveillance in the Municipality Act (*Gemeentewet*) and general data protection law, no specific provisions regulating other types of surveillance used by the municipality or private actors exist. It would be interesting to see, whether the

390 In the case of an Article 8(2) assessment, the Court would easily and quickly conclude that the surveillance follows a legitimate aim, likely that of crime prevention and maintenance of order. In the case of positive obligations, the Court would do a balancing test between the private life interests of the applicant and the interests of the other party (e.g. protection of private property, in this case connected to public order interests).

Court would find data protection law sufficient for the regulation of these various technologies employed in public space. It is difficult to speculate about this, but one might point out that given the potentially serious intrusion into one's private life, it would be desirable for the Court to require another or complementary legal framework with additional safeguards, more specific to the surveillance context at hand.

Nonetheless, even if the Court would find the measures in accordance with the law, it would still need to examine whether they are necessary in a democratic society. It is particularly at this step that the two tests (Article 8(2) and positive obligations) come closest. As such, I will generally examine the types of factors that the Court might consider. Even in the case of requiring only the basic safeguards concerning a lesser intrusion into private life, the Court might determine in the *SLL* example that: (1) surveillance is deployed in a semi-covert manner (while it is certainly no secret what is happening on Stratumseind, there is also no sign on either side of the entrance to the street and, moreover, the extent and particular operation of surveillance is very much unknown to the public); (2) surveillance is deployed indiscriminately, rather than following concrete suspicion; (3) surveillance is deployed continuously, including continuous storage and aggregation of data without clear limitations; (4) there might be less intrusive measures possible and available in order to reach the same aims (also possibly concluding that the employed means are not – or not the best – suitable means to go about the goals at all); and (5) there is not sufficient notification of the surveillance taking place.

A longer assessment would, of course, be needed in order to speculate about the case with more authority. Nevertheless, the above brief assessment seems to at least suggest the possibility that the Netherlands would be found breaching its positive obligations (as it had not struck a fair balance between the opposing interests) or that the measures employed are not in accordance with the law or necessary in a democratic society.

7

CONCEPTUALISING PRIVACY *FOR* PUBLIC SPACE AND SUGGESTIONS FOR REGULATION

An outline

1. INTRODUCTION

From the end of the 1990s we can observe privacy scholarship moving away from accounts of privacy understood as 'personal privacy' that has value only for the individual (disengaging her from social and political life), to an account, according to which privacy has great value *also* for society and democracy more broadly. This can be seen as yet another development of the word and notion 'private', which has been evolving ever since its conception in the 14th century (Williams, 1983, p. 242). One can thus argue alongside Williams, that privacy (connected to the notion 'private') retains the multiple meanings arising from its long tradition, however, a particular meaning might be predominant at a certain place and time. While the predominant meaning today is still that of 'personal privacy', my aim in this dissertation and this final Chapter is to further the scholarship emphasising its broader societal and political value, and to do this in the particular context of privacy in public space.

The examination of the types and techniques of surveillance within the *Stratumseind Living Lab*, the particular privacy-related risks stemming from them, and the level of legal protection granted to privacy in public space by Article 8 ECHR in the previous chapters have resulted in a deeper understanding of the complex issues that are at the focus of this dissertation. In this final Chapter I am thus well-equipped to answer the main research question: *how can and should we conceptualise privacy in public space in the context of surveillance in smart cities and living labs?*

Based on the analysis in previous chapters, it can be seen that the values, dimensions and mechanisms of privacy in general (at least as a theoretical concept) broadly fit and warrant protection of privacy in public space. Several contemporary privacy scholars conceive privacy in a broad manner as an infrastructural condition and right (e.g. J. E. Cohen, 2017; Koops, 2018), which has value not only for the individual but for society and/or democracy more broadly (e.g. Gutwirth, 2002; Hildebrandt, 2006b; Mokrosinska, 2018; Nissenbaum, 2010; Regan, 2015; Roessler & Mokrosinska, 2013). The definition that I employed in this dissertation (privacy as breathing room for socially situated subjects to engage in the processes of boundary management through which they define and redefine themselves as subjects; J. E. Cohen, 2017) is generally broad enough to encompass the various risks stemming from surveillance of public space as seen in contemporary smart cities and living labs.

However, these accounts are also very abstract, offering few concrete suggestions or starting points in order to be applied, especially in law. In this sense, I posit that privacy in public should not simply be treated as privacy in private (as Allen argues;

1988, pp. 123–124). As I have shown in Chapter 5 in particular, the specific context (or manifestation) of privacy in public space in connection to surveillance within living labs and smart cities, comes with a particular focus of its own – that is, on the social and political aspects of privacy, which are in line with the values of sociability and political participation connected to public space. As such, privacy and public space have a functional relationship as I will show below. On the one hand, the protection of privacy serves to protect those aspects of public space connected to political participation and sociability. One the other hand, the protection of these same aspects of public space also serves to protect certain aims of privacy. In other words, privacy and public space go hand in hand. Therefore, one should not only think of possibilities for preserving the *privateness* in public space but also about preserving the *publicness* of public space.

What is needed then is a more concretely situated description – in fact, conceptualisation –, which would allow for the emergence of new elements and strengthened arguments in the analysis and, thus, a better appraisal of the concept.

The general aim of this concluding Chapter is, thus, synthesis. I attempt to draw together key threads of discussion throughout this dissertation, combining perspectives of privacy and public space (and, to a certain extent, surveillance) in order to explore how privacy in public space can and should be conceptualised so as to also address the social and political significance of public places. Such analysis would then provide a more solid foundation for the regulation of surveillance there. To echo Jenkins (2014, p. 50), the apparent mutual ignorance of the various disciplines at play – as might have occasionally become clear throughout the chapters – sometimes irritated me. My goal in this dissertation then can be described as a synthesis of insights from different disciplines that is greater than the sum of its parts; to provide a theoretical framework within which the private and the public (in the form of privacy in public space) can be understood as going hand in hand, rather than as opposing themselves.

As I point out below, simply put, conceptualisation is a way to organise thinking about something and to represent it for others to see. As such, I should point out that I am clearly building on existing work, particularly the work of privacy scholars mentioned above. What is original in this Chapter, however, is the particular way in which I organise these thoughts and which, I posit, might lead to a better understanding of what is at stake in the context of privacy in the public spaces of smart cities and living labs. I argue that rather than speaking of privacy in public space (PiP) an account of privacy *for* public space (PfP) should be developed. That is, an account that would be

better equipped to address the risks both for the particular aspects of privacy as well as those of public space that are at stake with networked surveillance.

I should also point out that the particular issues stemming from smart city surveillance of public space might well be conceptualised and regulated in other ways. I am not claiming that the sole way of going about them is through (the rights to) privacy or that this approach will solve all of the interconnected issues, which I have called privacy-related risks. Not at all. There are other possible ways of approaching the matter, such as strengthening the freedom of assembly and association, the freedom of expression (especially in relation to issues of surveillance and its impact on political manifestation; similarly Aston, 2017), the right not to be subjected to discrimination and similar. In fact, I posit that these various approaches should be working together, which is connected to the infrastructural condition of privacy, which serves other values and rights (see Chapters 3 and 5). However, the approach through privacy has a notable strength, which others do not possess – it is high up on international and national agendas, where the accepted claim is that privacy (and data protection) need to be taken seriously. As such, further research in this area might more likely (although perhaps still not very likely) lead to regulatory change. This is, of course, a pragmatic argument, fitting rather well with the general approach of this thesis, which follows the pragmatic philosophical path, beginning its academic assessment with a concrete problem found in the illustrative example of the *Stratumseind Living Lab*.

My concern in this Chapter is, thus, not only conceptual. I attempt the conceptualisation first and foremost in order to have a better understanding of the nature and value of privacy interests in public space, as this is essential for the development of effective privacy regulation in this context. As such, in the second part of the Chapter I open up the discussion by briefly examining the possibilities for regulation of surveillance of public space within smart cities and living labs, employing Morgan and Yeung's (2007) five types (or Cs) of regulation: Command, Competition, Consensus, Communication, and Code. In this last part of the Chapter, I come back to the beginning part of my dissertation – the *Stratumseind Living Lab* –, positing that the *SLL* itself is a hybrid regulatory tool, trying to combine competition, communication and consensus types of tools. This regulatory tool, as I have shown in my analysis in Chapter 1, however, comes with several shortcomings and is in need of regulation of its own. I conclude that there is a need for a combination of various tools of regulation, if the possibility of achieving privacy *in* or, rather, *for* public space is to be achieved and preserved in the new environments of living labs and smart cities. In particular, a combination of tools of consensus, communication, code and command is needed.

The concluding Chapter is structured in two main parts. The first part begins with a description of the particular type of conceptualisation employed – conceptual combination, in which a 'head' concept is combined with a 'modifier' concept. This is followed by the conceptualisation of 'privacy *for* public space' based on the method of conceptual combination. First, I discuss the relevant dimensions of the head concept of the combination, i.e., privacy. Second, I briefly discuss the specific context relevant for this conceptualisation, that is surveillance as found within contemporary smart cities and living labs. Finally, I identify the relevant dimensions of the modifier of the combination, i.e., public space, which I then apply to the head concept, resulting in a rough outline of the newly formed concept 'privacy *for* public space'. In the second part of the Chapter I offer a brief discussion of possible tools and measures for regulation of privacy (or, rather, surveillance) in public space within living labs and smart cities. I end this Chapter and the dissertation with a final conclusion.

2. THE PROCESS OF CONCEPTUALISATION

This is a first attempt at conceptualisation and, as such, I am referring to the *process* of conceptualisation (conceptualising) rather than to the end of the process (conceptualisation itself). My aim here is to offer some initial ideas for future conceptualisations of a more robust understanding of privacy in public space, aimed at better addressing the risks stemming from previously insignificant sources (public places, public activities and public data) and applying to previously hardly (or non-) applicable areas – groups and social and political participation.

2.1 A note on conceptualisation

If concepts are constituents of thought (Margolis & Laurence, 2011), then a concept of *privacy in public space* is needed in order to properly think about, that is examine, the need, value, meaning and protection – or lack thereof – of privacy in public space.

As we encounter new things or phenomena in the world, we form conceptual representations of them in an attempt to understand them (Kahl & Yates, 2009). In other words, we conceptualise them. Sometimes this happens rather instinctively (especially when dealing with simpler things, such as a newly invented vehicle, which comes to be known as a bicycle), while at other times conceptualisation requires serious research and creative effort. The latter is the case when dealing with complex and abstract notions, such as with the issue at hand.

Conceptualisation can be defined as 'an interpretable arrangement of concepts and/or entities' (Trochim & Linton, 1986, p. 290).[391] Similarly, in information science conceptualisation has been defined as an abstract simplified view of some selected part of the world, containing the objects, concepts, and other entities that are presumed of interest for some particular purpose and the relationships between them (e.g. Genesereth & Nilsson, 1987). Simply put, conceptualisation is a way to organise thinking about something and to represent it for others to see.

Of course, people often develop different conceptualisations of the same new matter. For instance, Pinch and Bijker (1984) have shown how some groups interpreted the bicycle, when it first appeared on the market, in terms of safety, whereas others focused on speed. This is connected to the fact that different groups fit the new concept within different existing beliefs and conceptions, trying to create a coherent picture of the world or its part (DiMaggio, 1997; Durkheim, 2001, pp. 333–334). Furthermore, there are various ways to conceptualise, for instance through analogy or classification, which lead to somewhat different understandings of a concept. Analogy, for instance, maps the relational structures between concepts and highlights similarities. Classification, in contrast, focuses on highlighting differences (Kahl & Yates, 2009, p. 4). This is to say, conceptualisations are not objective representations of things or phenomena; rather, they reflect the choices that we made in its course.

This also applies to my own conceptualisation of privacy in public space, which is placed within a particular context of contemporary privacy scholarship, seeing privacy as a broad concept, valuable for the individual as well as for social interests, and a human right. For reasons that I explain in the next Section, I have chosen to employ a 'conceptual combination' approach.

2.2 Conceptual combination

Conceptual combination is 'a fundamental process of human cognition, in which people use two or more concepts to articulate and comprehend complex meanings that a single concept cannot denote' (Ran & Duimering, 2010, p. 86). We regularly use conceptual combination in order to develop new ideas and communicate with one another. In everyday language, for instance, words are continually combined into phrases of this sort in the making of sentences. Conceptual combination is found in vastly different instances, from Shakespeare's evocative characterisation

391 Generally, entities are understood as more restricted units of meaning than concepts (concepts may be either individual entities or groups of entities), which are in turn more restricted than conceptualisations (Trochim & Linton, 1986, p. 290).

of parting as 'sweet sorrow' to more recent attempts of boosting the sale of rather expensive automobiles by using a contrastive combination such as 'affordable luxury' (Ward, Smith, & Vaid, 1997, p. 6). Moreover, the ability to combine concepts plays a fundamental role in the expansion and structuring of knowledge and has been recognised as valuable in the context of philosophical investigations and the phenomenon of scientific concept development (Thagard, 1984). Such combination produces a new concept as a non-linear and non-definitional amalgam of existing concepts (*ibid*., p. 3).[392] In simpler terms, merging two or more concepts can result in a novel entity that is more than the simple sum of its component parts. I use conceptual combination in this last sense, as a guiding principle in the development of a new complex concept.

As I am not inventing a new concept out of the blue, rather, I am attempting a novel conception of privacy in a particular context, it makes sense to anchor the new concept within a familiar existing one. In fact, it makes sense to anchor it within two familiar concepts – privacy and public space (see Chapters 3 and 4). Just as with definition, conceptual combination forms new concepts from old ones, but employs a more flexible and complex mechanism. It acknowledges that more complex processes are required because there is more to concepts than just necessary and sufficient conditions, which can be summed up to produce new concepts (Thagard, 1984, p. 4). Concepts may, namely, have conflicting expectations which the combination will need to reconcile. This is precisely the case with privacy in public space, where the private and the public are commonly considered opposites. According to Rothenberg (1995, p. 433), much creativity results from simultaneously holding in mind two opposing concepts, a process that he has termed 'Janusian thinking'.[393] Conceptual combination then seems a rather fitting approach to conceptualising privacy in public space, where the two notions are traditionally seen as opposites.

In conceptual combination, two concepts are generally combined: one is referred to as the 'head' and the other the 'modifier'. The head concept refers to the central concept in the combination, usually corresponding to the second word in the combination in English (the head of the noun phrase in syntactic terms, thus giving it its name). The modifier refers to the concept in the combination that changes some aspects of the head, usually corresponding to the first word in the combination in English (Ran &

392 Whereas a linear and definitional amalgam of existing concepts shares all of the characteristics of the original concepts (e.g. a combined concept of 'red apple' shares all of the characteristics of an apple and the colour red), that is not the case with non-linear and non-definitional combinations.

393 A reference to the Roman deity Janus who had two faces pointing in opposite directions.

Duimering, 2010, p. 85). For instance, in the concept of a 'mixed blessing', 'blessing' is the head and 'mixed' its modifier.

In the case at hand, privacy corresponds to the head concept, while public space corresponds to the modifier. While a combination of two concepts commonly results in a combination of two words, it is clear that concepts exhibit a greater variety of linguistic manifestations than just nouns, including adjectives, verbs, prepositions and adverbs, which deserve an equally rich representation of their conceptual structure (*ibid*., p. 86). In the case of 'privacy in public space', we are experiencing syntactic constraints that do not render other equally satisfying possibilities. 'Public-space privacy' would, in principle, be possible, however, besides being an unusual combination, it less informative at first sight than 'privacy *in* public space'. Some privacy scholars, including Westin (1967) and Slobogin (2002), have used the term 'public privacy'. By dropping 'space', the concept becomes broader (referring to the public sphere in general) and comes to include issues concerning public information and digital public space, oftentimes focusing on informational privacy. Privacy in public space, instead, focuses on physical public spaces, where types of privacy other than information are also very relevant (including associational and behavioural privacy; see Koops et al., 2017). This is important, since focusing on the spatial setting of privacy helps to remind us that privacy is a condition of human beings and that humans are embodied beings, living in four-dimensional space/time (Koops, 2018). Furthermore, as Cohen (2012, p. 109) has observed, the insistent recurrence of spatial metaphors for privacy 'suggests that something about the experience of privacy, and that of privacy invasion, is fundamentally and irreducibly spatial'. In fact, as I will explain below, the combination that I have chosen is 'privacy *for* public space'.

Of course, there is wide diversity of ways in which concepts can be combined and researchers from various fields, including cognitive psychology, linguistics, artificial intelligence, and philosophy, have proposed several models of conceptual combination. Whereas in most theories of conceptual combination the head dominates the meaning of the concept,[394] I will employ an approach, according to which both the head and the modifier contribute more or less equally to the meaning of the new concept.[395] In this case, the modifier and the head play different but equally important roles. Generally,

394 In selective modification, concept specialisation and dual-process model the head dominates, while in the CARIN model the modifier dominates. In the interactive property attribution model both contribute equally to the meaning; see (Ran & Duimering, 2010, p. 85).

395 The 'interactive property attribution model' (IPA) model, for instance, follows this approach (Estes & Glucksberg, 2000).

the head provides relevant dimensions and the modifier provides candidate properties for attribution. For example

> 'in the combination *shark lawyer*, the head concept lawyer provides relevant dimensions for attribution (e.g. TEMPERAMENT, COMPETENCE, COST, etc.), and the modifier shark provides salient candidate properties (e.g. "predatory," "aggressive," and "vicious") that can be attributed. … [I]n the [IPA] model …, instead of exhaustively aligning the dimensions and comparing the features of the two concepts, people align the relevant dimensions of the head with salient properties of the modifier' (Estes & Glucksberg, 2000, pp. 29–30).

This approach is particularly suitable for my conceptualisation of privacy *for* public space, in which I posit that privacy and public space have a special functional relationship, connected to social and democratic functions of privacy, where privacy in public space also serves to protect certain aspects of public space connected to political participation and sociability.

Conceptual combination can also involve combining concepts at the attribute level, the relational level or both (Wisniewski & Love, 1998). For the same reasons as stated above, I will employ both an attribute and relational approach, combining the concepts based on the chosen attributes, which depend on a particular relation between the modifier and the head noun (Shoben & Gagné, 1997, pp. 31–32). The selection of the relation is key and is, according to several scholars, importantly determined by context (Clark, 1983; cf. Murphy, 1988). This means that the relationship also depends on the dimensions of other concepts that are salient at the relevant moment (Murphy, 1988).

In the case at hand, the context that needs to be taken into account is surveillance, in particular the types and logics of smart city surveillance as I have identified them in Chapter 5. As I have pointed out in previous chapters, surveillance changes the relationship between privacy and public space. Firstly, surveillance technologies blur spatial and temporal bounds of particular social contexts (e.g. persons' movement, facial expressions and company are not only detected but also stored as data, analysed and potentially used to make decisions), making it very difficult for persons to actually achieve privacy *in* public space (as was still possible in the recent past). Secondly, contemporary surveillance within smart cities (but also more broadly) increasingly targets persons as parts of a group (often an algorithmic group) rather than as individuals. While persons might not be individually identified, they are nonetheless reachable. Furthermore, contemporary smart city surveillance achieves this and generally operates through changes in the architecture of public space, embedding

software (code) into it. This in turn affects the texture of public space itself, making it less conducive to sociability and political participation – two fundamental features that make a place *public*.

For these reasons, I have chosen the relational category 'for' in order to conceptualise 'privacy *for* public space'. In particular, the 'for' in privacy *for* public space stands for both the dimension of privacy best suited to this particular context and the role of privacy in facilitating the social and political properties of public space. In the next section I will thus employ this type of conceptual combination in order to sketch an outline of privacy *for* public space.

3. CONCEPTUALISING 'PRIVACY *FOR* PUBLIC SPACE': A ROUGH OUTLINE

3.1 The head: 'self-development' as the relevant dimension of privacy

For this conceptualization I employ the typology of privacy by Koops et al. (2017; see Image 7 on p. 96). Based on the discussion in Chapter 5, I have determined that associational and behavioural privacy represent the two types of privacy that are most relevant in the context of (semi)public space (alongside informational privacy, which is an overlay dimension of all types of privacy). Examining the chosen privacy typology, one can determine the most relevant dimensions of privacy in public space. On the axis of social interaction, the most relevant dimensions of privacy in the context of public space are clearly the 'public zone' and, to a certain extent, the 'semi-private zone', particularly in regard to semi-public spaces such as the emergency ward of a hospital or a large lecture hall. On the axis of freedom, the dimension of self-development, that is the freedom to act autonomously in public space (within the broad boundaries of social and legal acceptability) is most relevant (this also follows from Chapter 6). Negative freedom (that is, the capacity of people to ward off interference by others) might also be implicated, however, this capacity is generally quite limited in public space, where we are always potentially exposed to others. Since the public zone will play a key part as the modifier in this conceptual combination, I have chosen self-development as the most relevant dimension of the head concept.

The focus of privacy in public space is, thus, on self-development. Although one can find solitary places outside of the home and one can desire to be let alone whilst among others in public space (for example, by avoiding eye contact with others and immersing oneself in the acoustic cocoon of one's headphones), privacy in public space does not focus on disengaging the individual from social and political life,

despite persistent claims of the traditional liberal perspective on privacy. Quite the opposite, privacy in public space focuses on facilitating an autonomous development of one's identity and, related to that, a broad range of social relations (particularly "secondary relationships", as they are called in sociology; Lofland, 1998), including political associations.

A substantial part of identity is, thus, developed in (semi-)public venues. This is connected to the fact that individuals are not prior to social groups – each person exists *in and through* their interaction with them (Hildebrand, 2008, p. 111). One thus becomes an individual by virtue of social engagements with communities. As Dewey (MW15, p. 176; as quoted in Hildebrand, 2008, p. 111) put it, '[o]nly in social groups does a person have a chance to develop individuality.' As such, sharp lines between self/society and self/other are erased; instead these elements are understood as dynamic, ongoing events.

The way individuals generally form such relations is through social norms and behaviours regulating relations in public, such as civil inattention and reserve (see Chapter 4). These norms of interaction are necessary conditions of the functioning of all interactions (Roessler & Mokrosinska, 2013, p. 12). They allow persons to put forth different versions of themselves in different contexts (Goffman, 1959), allowing them to show themselves differently to their fellow barflies, regular taxi-drivers and to strangers sitting next to them on the tram. This 'audience segregation' (as it is called in sociological research) serves the purpose of self-*production*, as a part of our anticipation, rejection or acceptance of others' assessment of us. Adequate self-realisation, including the realisation of this myriad of roles, thus requires a certain level of privacy in public, which enables us to present to others only those parts of ourselves that we want them to see (Sloan & Warner, 2015).

Contemporary surveillance practices within the *SLL*, however, affect these processes by blurring the spatial and temporal boundaries of persons' experience in public space. Because of networked surveillance persons can no longer properly adapt their behaviour based on their expectations of others' observing them in public. In other words, they can no longer 'read' the social context and make out the social norms. While people might still be practically obscure and inconspicuous in relation to (most) other individuals in public space, who still treat them with a level of discretion,[396] this

396 Some people might be making secret recordings of others, for instance in the acts of 'upskirting' and 'downblousing' (see B. J. Koops et al., 2018) and posting these online or reporting them to the police (e.g. via the *Trillion* app).

is no longer so in relation to those *behind* the surveillance technologies. Nissenbaum's contextual integrity framework considers this in detail (2010).

Secondly, new forms of surveillance technologies also (try to) directly affect our behaviour in public space through various forms of nudging (as discussed in more detail in Chapter 5). As such, they potentially negatively affect our autonomy. Moreover, as I have shown in my analysis in Chapter 5, smart city surveillance increasingly surveils (and governs) us not as individuals but as a multiplicity – a group (both as a group present at a particular location, the Stratumseind street, and as an algorithmic group, e.g. a person at higher risk of aggression). In this sense, proliferating surveillance in public space may also negatively affect other rights and freedoms, such as the freedom of assembly and association.

3.2 The modifier: attributes of public space as a space of sociability and political participation

In order to combine the two concepts, certain properties of public space need to be attributed to the relevant dimensions of privacy. It should be noted, that I am speaking here of open or multiple-use public space (e.g. parks, public streets, sidewalks), rather than specified-purpose public space (such as railway stations or airports), where specific regimes might be in place. The way these properties are to be attributed to the relevant dimension of privacy is through the relational category 'for', as I explained above.

As follows from previous chapters, especially Chapters 4 and 5, sociability and political participation are the most relevant dimensions of public space in this context. I should point out that these are ideological constructions and contested ideals. And as such they offer valuable guidance. I will first discuss attributes connected to the sociability dimension of public space, followed by a brief discussion of relevant attributes of the political dimension. In order not to repeat what has already been discussed extensively in Chapter 4, I will mention the relevant attributes below only briefly.

3.2.1 Attributes of sociable public space

Forming more or less loose and minute relations with others in physical public space is valuable not just for the social identity of the individual but also for the social life of the community (Zukin, 1995). As I have discussed in Chapter 4, by providing a place for diverse groups to mix, public places afford people with face-to-face interaction and opportunities to participate in informal community life. Such public space is thus embedded with values of plurality, openness and social learning, making diversity agreeable or, at least, manageable. This is possible with the help of social norms,

which facilitate the development of trust. Such trust is essential for communal life, promoting social integration. Jacobs (2011, p. 73) offers an illustrative description about how such trust among strangers comes to life:

> 'It grows out of people stopping by at the bar for a beer, getting advice from the grocer and giving advice to the newsstand man, comparing opinions with other customers at the bakery, … admonishing the children, hearing about a job from the hardware man, … admitting the new babies and sympathising over the way a coat faded. Customs vary: in some neighborhoods people compare notes on their dogs; in others they compare notes on their landlords.'

While most of these relations in themselves are utterly trivial, its sum is not trivial at all. Such trust is born out of social interaction with strangers and, importantly, its cultivation cannot be institutionalised (*ibid*., pp. 73-4). However, social norms can also – and indeed do – function in a repressive manner, stifling social difference (see e.g. Mill, 2016). A delicate balance is at play here.

Sociable public space thus has and requires several characteristics. Most notably, it is a space of open access, where no person or group has exclusive control over it. It is also a space where there is flexibility of use, which allows for a fluidity of negotiation. Diverse groups and types of persons first need access to public space and an opportunity to behave there as they see fit (within the general bounds of the law). As such, public places force us to engage with 'otherness', going beyond one's personal boundaries. In open and accessible public spaces, as Young (1990, p. 110) put it, 'one should expect to encounter and hear from those who are different, whose social perspectives, experience and affiliations are different.' Following Sennett (1992b), a certain level of disorder in public space is thus healthy. Without it, people do not learn to deal with conflict, so that when conflicts do arise, they might be more violent. Sociable public space is thus also a space that allows for a certain level of disorder.

The four main attributes of sociable public space can therefore be summed up as: open access, absence of exclusivity of control, flexibility of use and allowing for a certain level of disorder.

Contemporary digital surveillance in public space, as can also be seen from the *SLL* example, affects these properties of public space, particularly within the wider transformation of public space into privatised and securitised space (see Chapter 4, Section 4). First, it transforms multiple-use public space into a space with a much

more narrowly defined purpose. Most often, this purpose is consumption, either in the sense of beverages, shopping or similar. Types of activities that are not conducive to consumption (ranging from sitting on benches to street performances) are either directly prohibited or discouraged (e.g. through nudging). In line with this narrowing down of use, openness of access is often limited too. Persons who are considered 'bad customers' (e.g. youth or poor people) or are not seen as customers at all (like the homeless) are likely to be excluded.

Connected to this is the possibility to encounter and develop numerous different types of social relations in public space. When a space becomes tailored to a particular type of group (e.g. hipster youth and upper-class shoppers), this possibility becomes very limited. Finally, contemporary public spaces are said to be ever more tightly scripted, that is, disorder is attempted to be eradicated from them. This can nicely be seen from the *SLL* example, where 'escalated behaviour' is defined in such a broad way ('all types of behaviour of persons who in some way lose self-control, including screaming, getting abusive, aggressive or crossing other behavioural boundaries that a person would otherwise not cross') so as to exclude a multitude of behaviours that have until now, for instance, been seen as merely eccentric or rude. If this understanding of escalated behaviour and its mission (to de-escalate it) would be taken very seriously, such space might come to allow only a very low (and 'unhealthy') level of disorder.

3.2.2 Attributes of political space

In relation to politics, public space provides individuals and groups a material space to engage in face-to-face political participation, essential for the creation of multiple publics (D. Mitchell, 2003; Young, 2000). According to Arendt (2006), democratic society needs to foster the plurality of identities, voices, and perspectives represented in their multiplicity in the public arena. Only through the various others that are co-present in public space, can persons perceive the world in its many perspectives, thus allowing for an agonistic – that is polemical but inclusive – co-existence (see Mouffe, 2013, 2014). These multiple public spheres (or publics) have a double function: on the one hand, they enable persons to form common opinions and arrive at common decisions; and, on the other, they allow for a multiplicity of sometimes contending ideas and claims. Their effect is thus the possibility of developing different responses to social issues, where the possibility of conflict plays an integrative role. In this sense, public space has been called 'open-minded' (Berman, 2006).

Public space as political space is thus a place for the exercise of 'personal rights that are both politically and spatially grounded, including the right to representation, assembly and freedom of action in urban open spaces' (Koops & Galič, 2017, p. 31).

In order for persons to have the possibility to exercise these rights, open access to public spaces is required. Secondly, it requires that no one group or person can claim control over a public place. For instance, a person or group does not have the right to exclude another person or group from public space for wearing a burqa or for being or showing behaviour associated with LGBTQ+.

A particular attribute of political public space is found in the possibility to express dissent. Citizenship, namely, not only consists of formal political rights granted by the state (the right to vote, to speak freely, to assemble and so on), it is also a social practice that brings together complex identity politics and power dynamics (D'Arcus, 2004, p. 357). This is also connected to the fact that publics are performed, constructed and fabricated, rather than given (Dewey, 2016); in fact, their articulation and assemblage require hard work (Hildebrand, 2008, p. 186). In this sense, dissent as an important practice of citizenship plays an important role. Dissent relates to 'ongoing, everyday micro-struggles within specific locales in which ordinary people use resources at hand to make small "tactical" raids upon the different ways in which our lives are governed' (Roberts, 2008, p. 655; referring to De Certeau 1984; Harvey 1996; Merrifield 2002). Everyday dissent thus includes active resistance (e.g. riots and protests) but is broader than that, including the possibility to dress differently (e.g. punks), vent out complaints and hold a sign at a street corner and distribute flyers for a cause.

However, the value of public space in regard to the making of claims lies not only in the possibility to participate (thus requiring open access) but also in the possibility of being seen. While in some cases (e.g. in the case of trying to inform the publics of a particular personal 'injustice') persons seek individual identifiability (as found in our passports; *idem* identity), another type of visibility needs also to be possible. That is a type of visibility, which allows for one's voice to be heard without leading to repercussions on who voices it. That is, political activity oftentimes requires anonymity (keeping the *idem* identity hidden). Anonymity is important to ensure that protesting citizens can be themselves as political agents. The freedom to protest as a political actor namely requires freedom from others' judgement that would implicate other parts of identity (Koops, 2018).

The four main attributes of political public space can thus be summarised as: open access, absence of exclusivity of control, allowing for dissent and for a certain level of anonymity.

As with sociable space, widespread untargeted surveillance of public space affects the attributes of political space. First of all, by granting businesses the power to develop

and operate surveillance technologies in public space (in particular, for instance, to determine what is considered escalated or aggressive behaviour), municipalities are granting these businesses the possibility to determine what is the public interest and to control public space. This is particularly problematic, when it is done without a higher level of participation (in the sense of Arnstein's participatory ladder; 1969) of the residents of the city.

As mentioned in the previous Section, public spaces are being transformed into spaces conducive to consumption. From this 'corporate' perspective, conflict (an important part of dissent) is not good for consumption and is seen as something to be eradicated from public space. In contemporary cities, dissent is not only managed through the regulation of the time, place and manner of (protest) gatherings (e.g. requiring a permit), dissent itself (as with disorder more broadly) can be said to be perceived as escalated or inappropriate behaviour, which needs to be diffused or excluded. As I have discussed in Chapter 5 through hypothetical scenarios, protest can thus be discouraged through the use of various types of nudging and surveillant technologies.

Furthermore, the increasingly sophisticated and pervasive surveillance technologies are making the possibility of being anonymous in public space very difficult. Wearing a hoodie or a hat that hides parts of your face from other persons matters little to the wide-angle and zoom-enabled video camera with embedded capabilities of facial recognition or gait detection, where the contours of one's chin, nose and cheekbones or the way one walks are enough to single her out and identify her (especially when connected to data gathered from other sources, such as one's MAC address and mobile subscription).

3.3 Integration: privacy *for* public space

Based on this conceptual combination the six identified attributes of public space need to be attributed to the self-development dimension of privacy. These attributes are: (1) openness of access; (2) absence of exclusivity of control; (3) multiple use; (4) tolerance of a level of disorder; (5) anonymity; and (6) allowing for dissent.

As discussed above (and, more extensively, in Chapter 4), the self-development dimension of privacy in public space shows that for individuals to develop into autonomous beings, both personally and politically, they need to venture out of their private spaces into public space and interact with others. That is, they need to form various social relations with strangers and near-strangers and participate politically in public space. In other words, persons need to be able to participate in the informal life of the community as well as in the formal civic life of the public spheres. As

has already been acknowledged in privacy theory, privacy thus needs to protect the possibility to develop and maintain social and political relations, which, it argues, has value not only for the individual itself but also for society and democracy more broadly.

My conceptual combination strengthens this point but goes further. According to this conceptualisation, in order for a person to be able to develop herself in such a way, certain attributes of public space itself should also be protected. The first two attributes relate both to public space as sociable space and as political space. First of all, access to public space needs to be generally open (although it can also be narrowed down, if special circumstances demand it). For one to participate in communal and political life in public space, one first needs to be allowed to access it. And secondly, no single person or group may claim control over the public space. For example, nudists cannot claim the nicest part of the public beach and exclude non-nudists or confront them with their 'Adam and Eve' costumes. Businesses alike cannot claim control of public space, determining who can enter and which types of activities can be performed there.

The following two attributes relate specifically to the possibility of persons to develop multiple types of social relationships with others and, in turn, to contribute to the sociability of public space. There needs to be a flexibility of use in public space that is not a designated-use type of public space (e.g. airports, libraries). In order for a person to be sufficiently free to do what she wants, and thus to develop herself in an autonomous way, use should not be prescribed too strictly. For instance, one should be able to linger carelessly on a street without buying anything or to sing to oneself out loud, even if out of tune. Furthermore, in order for a public place to be sociable, a certain level of disorder needs to be tolerated, in fact it should be seen as central for its functioning. Places where the rules of conduct are too tightly scripted, orderly and safe (trying to make visitors feel 'too comfortable'), might make one feel better in that particular moment, for instance by not making her feel distressed by the sight of homeless persons or addicts. However, they do not lead one to further develop as an individual person and a member of society (e.g. prompting one to support organisations that volunteer with a local homeless shelter or help to integrate former addicts back into society). If one is not confronted with different parts of social life, including or especially those that make one feel uncomfortable, persons may become separated from differing aspects of social life, effectively isolating them in their own cultural or ideological bubbles (a type of offline 'filter bubble'; Pariser, 2012). Furthermore, it might make people feel bored, which is not desired particularly in regard to city centres and nightlife streets, where liveliness is sought to be preserved.

By filling in the properties of sociable public space with the self-development dimension of privacy, one can determine that in order for an autonomous individual to develop, there is a need not only for a 'room of one's own' but also for a public space, where a certain level of trust reigns, into which an individual may and must venture and where she feels – and actually is – sufficiently free to behave and perform according to her own wishes. One might call such space 'a street of our own.'[397] As I have argued in Chapter 4, spaces and social life are made through emergent patterns of use, their individual and social functions, and power relations. As such, it is vital to protect public space as shared space, with mutual rights and responsibilities, rather than as a realm where privacy and other individual rights are subject to the whim of others, in particular the state and corporations. Therefore, by adding this dimension to the concept of privacy, the argument for protection of privacy in public space is strengthened. Such an enriched dimension more clearly expresses the social value of privacy and why it needs to be protected.

The last two attributes are connected to the possibility of persons to develop as autonomous political subjects (that is, fully-developed citizens) by having the possibility and opportunity to participate in political activities in public space, to develop political relations and form multiple publics. In order for this to be possible, achieving anonymity in public space needs to be possible, even (or especially) in an age in which its extinction seems possible. Moreover, the possibility of expressing dissent in numerous little ways needs to be preserved; in fact, it needs to be encouraged.

As with sociability, forming political relations and participating in political activities has value both for the individual, who is developing herself into a political subject, as well as for a democratic society more broadly, which requires fully-formed political subjects and multiple publics in order to exist. By attributing the properties of political participation to the self-development dimension of privacy, the role of a certain type of public space in achieving this is expressed more clearly. On the one hand, the connection between privacy and public space has been well-described by Staeheli and Mitchell: 'Public space is not only a space of politics, it is also a space constituted *in* and *through* privacy' (2004, pp. 149–150). On the other hand, one should also state: certain aspects of privacy (particularly those relating to the self-development dimension) are in turn constituted *in* and *through* public space.

397 Azar Nafisi refers to a similar idea in her book, Reading Lolita in Tehran (2015, p. 12), when describing her living room in which she held a subversive private reading club, as a 'space of our own', that is, 'a sort of communal version of Virginia Woolf's room of her own.'

A vision of privacy *for* public space (PfP) thus allows us to better acknowledge the interconnectedness of the value of privacy in public space for the individual and for society and democracy more broadly. Such privacy, therefore, has a fundamentally Janusian form: with one side it looks towards the individual and with the other it overlooks society and democratic politics. However, rather than leading to opposition, these two sides work together and strengthen each other.

PfP also emphasises the connection between identity-development and place. It does not suffice to note that one becomes an individual *in* and *through* interactions with others; it is also important to point out that this commonly happens in public space with spatially grounded rights. As such, PfP furthers the recognition of the facilitative role of privacy in allowing for a more secure and fuller exercise of other rights and freedoms, in particular the right to representation, freedom of assembly and association and of expression. While this aspect of privacy has relatively recently been gaining support in privacy theory, it has as yet not been recognised in relation to privacy rights, including Article 8 ECHR (see Chapter 6).[398] As I have argued in Chapter 6, this would be a welcome development.

Because of its Janusian form, PfP can generally apply to both persons as individuals as well as to persons as a part of a multiplicity, such as an algorithmic group. In this latter sense, what is to be protected is not the privacy of any particular group (indeed, as Taylor, Floridi and van der Sloot (2017a) point out, algorithmic groups are fundamentally dynamic, which makes them difficult to pin down), rather the goal of such protection is the possibility to form associations and to behave autonomously itself – to develop oneself in an autonomous way. This is similar to the idea of Roessler and Mokrosinka (2013), according to which 'privacy of the relationship' should also be protected (alongside the privacy of the individual).

Privacy *for* public space therefore furthers the argument concerning the infrastructural role of privacy in enabling a more secure and fuller exercise of other values, rights and freedoms, such as the plurality, tolerance, freedom of assembly and association, and freedom of expression. And it does so by making more concrete *what* precisely is to be protected in order to preserve both the possibility for an individual to develop

398 The ECtHR recently had another opportunity to engage with these issues in the case of *Catt v. UK* (2019) Application no. 43514/15, a case concerning systematic (physical) police surveillance of protesters, including the keeping of files on individual protesters. While the Court did find a violation of Article 8 in the case, it decided so solely on the basis of recording of data relating to an individual's private life, not engaging at all in the relation between Articles 8, 10 and 11.

oneself in public space as well the sociability of and political participation in public space. This is an important task, especially as this aspect of privacy law has not yet been recognised in legal theory or case law.

4. REGULATING SURVEILLANCE IN SMART CITIES AND LIVING LABS

As I have shown in previous chapters, particularly in Chapters 5 and 6, the wide-scale deployment of surveillance within smart cities and living labs requires a regulatory response in order to preserve the possibility of privacy in public space. The protection offered by Article 8 ECHR is broad but also limited, particularly in the sense that it is in no way a quick remedy. Moreover, there are other types of regulation that need to be considered. The question then is, how to regulate?

Scholars have noted that an adequate regulatory response to a matter as complex as privacy requires stepping outside the frame of existing laws and regulations (e.g. Bennett & Raab, 2006; Katell, Dechesne, Koops, & Meessen, 2019 forthcoming). As Bennett and Raab (2006, pp. 117–118) put it, 'the interdependence of all of these instruments [including consent-building, communication and code] is what characterizes a privacy-protection regime as a whole.' Regulators should thus consider the whole repertoire of governance and regulation tools, and how these could and should apply to surveillance in public spaces of smart cities.

Regulation here is used in a broad sense so as to embrace a variety of instruments, rather than in the more specific sense of state or governmental activity involving laws and their enforcement by government agencies. In order to map out the possible tools for regulation in this context, I employ Morgan and Yeung's (2007) five 'Cs' of regulation: command, competition, communication, consensus and code. This heuristic device corresponds to the better-known regulatory toolkit of Lessig (1999)[399] but it allows me to differentiate between different types and functions of social norms: that is, communication tools and consensus tools. This additional differentiation allows for a more nuanced approach to regulation. While an in-depth analysis of the regulatory toolkit in relation to smart cities, living labs and privacy-related risks lies outside the scope of this Chapter, I offer some initial reflections so as to spur more in-depth discussions of particular tools, especially those related to additional legal tools, architecture and code.

399 Lessig's toolkit includes: law, market, social norms and architecture.

Before beginning with the analysis, it is important to note that the *Stratumseind Living Lab* (*SLL*) itself can be seen as a hybrid regulatory tool (employing a combination of competition, consensus and code tools), regulating social behaviour for the main purposes of safety and profit. However, as follows from the discussion in previous chapters, the regulation as currently employed in *SLL* is insufficient, as it leads to widespread and pervasive surveillance of public space and everyone in it. In this Chapter I thus argue that the existing *SLL* regulatory regime needs revision, in particular, it needs to be complemented with other tools of regulation (or forms of existing tools need to be changed). Moreover, the *SLL* itself needs to be regulated. I begin the discussion on how precisely this could or should be done by briefly examining those regulatory tools, which I consider less suitable and inadequate for the protection of privacy in public space (competition, consensus and communication), followed by a somewhat more extensive discussion on those tools, which I deem more suitable and promising for this task (command and code).

4.1 Five types of regulation

4.1.1 Competition, consensus and communication: limited possibilities for regulation

In this sub-section I will briefly examine three tools of regulation, which I consider less suitable and inadequate solutions for the protection of privacy in public space in the context of smart cities and living labs: competition, consensus and communication.

As stated above, the *SLL* itself can be seen as a regulatory tool partially based on competition – the market – employed for the purpose of controlling behaviour of persons on the Stratumseind street for the combined purposes of safety and profit. I base this assessment on the fact that key agents involved in the sub-projects of the *Living Lab* are private businesses and that the projects largely function by following the logic of the market (cf. Bennett & Raab, 2006, p. 117; see Chapter 1), rather than on the use of classical 'economic instruments' such as charges, taxes and subsidies (Morgan & Yeung, 2007, p. 85). Based on the logic of the market, 'technological solutions' for problems of safety on the nightlife street were sought to be developed (while other types of solutions were not considered) by the municipality co-operating with businesses (in public-private partnerships). As these technological solutions involve and are reliant upon a wide net of diverse and increasing surveillance technologies deployed throughout the Stratumseind street and beyond, they pose diverse risks related to privacy (and other values and human rights), both for individuals and society. As such, they are in need of regulation of its own, likely through types of tools other than competition.

One might imagine employing the classical types of competition tools, economic instruments, in order to regulate the use of such surveillance. This has been discussed in scholarship, particularly in the U.S., where there have been proposals to regulate informational privacy intrusions through market mechanisms similar to those in environmental law, such as environmental covenants, environmental management systems, environmental impact statements and emission fees (e.g. Froomkin, 2017; Hirsch, 2005). However, competition as a regulatory tool in relation to privacy, seems to have serious limits. Particularly in view of the development of social media and the platformisation of society, there are good reasons to be sceptical of market mechanisms (largely based on consumer choices) to protect information or other types of privacy as well as other threatened values. As Katell et al. (2019 forthcoming) put it: 'Particularly when it comes to shifts in power relations to the detriment of weak parties, the market is unlikely to redress the balance in order to better protect the weak.'

Another type of regulatory tool relies upon consensus and co-operation as the means through which behaviour is regulated. This consensual basis may derive its force from a legal contract or from social consensus, in which the community itself provides the primary mechanism through which control is to be exerted (Morgan & Yeung, 2007, p. 92). This latter type is particularly interesting for the *SLL*.

At least in principle, the *SLL* seems to employ social consensus as a regulatory tool alongside competition. This is based on the type of initiative that the *SLL* claims to be – a living lab. As I have discussed in Chapter 1, one of the key characteristics of living labs is that citizens/users are at the centre of innovation in order to develop technological solutions for the specific needs and aspirations of local contexts. Indeed, consensus as a regulatory tool is often used in relation to co-operative partnerships between state and non-state actors seeking to regulate social behaviour (*ibid*., p. 92), such as living labs and pilot projects more broadly. This sounds like a desirable type of regulation, however, in practice it does not always (or, rather, often) rely on actual consensus and co-operation. This is quite clear from the *SLL* example, in which claims of citizen participation were made often and realised rarely.

In 2015, Schreurs, the alderwoman of Eindhoven, commissioned a two-year collaboration between the city of Eindhoven and Het Nieuwe Instituut, a cultural institution, in order to add the citizen perspective to its transformation into a smart city (including the *SLL*), in particular concerning the changing relationship between citizens and the government (Vlassenrood, 2017, p. 8). However, this project showed that the debate about the smart city (or 'smart society', as follows from Eindhoven's

agenda) is still generally limited to data collection and restricted to insiders, based on data sets, representativeness of which is debatable (*ibid*., p. 10). Such an approach cannot be seen as being based on or building actual social consensus. Vlassenrood and other participants of the project came to several relevant conclusions. First, the city was thinking in terms of technological solutions at the outset, rather than trying to identify the relevant questions (including larger social issues), taking citizens' needs and desires into account (*ibid*., p. 17). Second, officials tasked with identifying the problems in a neighbourhood usually did so from behind a desk, based on 'hard data' (usually statistics). This approach, however, is not suited to identify more complex issues in society (such as loneliness and social cohesion), which cannot be adequately captured in data form. As such, 'hard data' should be enriched with 'soft information' (information gathered based on other methods, including 'unconventional' means) (*ibid*., p. 17). Finally, as Vlassenrood (2017, p. 9) concluded, 'the project has had less impact on the municipal agenda than we had initially hoped. Ultimately, there was insufficient linkage in terms of content and process'.

There are certainly other ways to go about consensus and citizen participation, but Het Nieuwe Instituut employed a wide range of innovative methods.[400] And while it is commendable that the Alderwoman of Eindhoven commissioned this project, its results should have had more of an impact on the city's agenda. In the particular context of the *SLL*, it is clear that the choice of means of improving the safety (and 'livability') on the Stratumseind street, was not done in any real co-operation with local citizens. As long as such insights carry no obligation to be taken into account, it is difficult to speak of consensus being used as a regulatory tool in this case. In view of such issues, it would be desirable to employ a hybrid technique, employing both command (law) and consensus tools. In this sense, the law might play a more prominent role in ensuring that citizen participation is taken more seriously (e.g. issuing guidance or directions concerning the ways in which public participation is to be achieved).

400 The project employed a wide range of unconventional and innovative tools, including gathering stories from local residents with the aim of identifying their needs, linking these stories to available data from the municipality and then discussing the findings in a series of workshops and talks with officials, designers, researchers and other citizens, devising follow-up actions (Vlassenrood, 2017, p. 12). In the 'Embassy of Data' exhibition, the project also created a 'data panorama'– a visualised picture of Eindhoven's efforts to become a smart city, particularly the types of data that are being collected, including the data captured within the *SLL* (see Becoming a Smart Society Embassy of Data. (2018). Retrieved March 31, 2019, from https://destaatvaneindhoven.hetnieuweinstituut.nl/en/activities-0/embassy-data).

Finally, communication-based tools (closely connected to consensus) regulate behaviour by enriching the information available to the targeted audience, thereby enabling them to make more informed choices about their behaviour (Morgan & Yeung, 2007, p. 96). In other words, this tool tries to influence persons' behaviour through rational persuasion. Concrete measures of such regulation include attempts to persuade or educate members of the regulated community or those affected by the regulated activity.[401] This type of regulatory tool, again, seems like a desirable method of regulating surveillance within the *SLL*. However, especially when it is not coupled with other regulatory tools, communication is often limited, disclosing little information or disclosing it in a way that is difficult to comprehend for lay citizens (e.g. in complex scholarly papers) or is useless without context (e.g. when it is presented in mere numbers in Excel sheets or other in incomprehensible '3D models', as in the case of the *SLL* data[402]). In the case of the *SLL*, as I have described it in Chapter 1, a very low level of communication with the general public can be observed, most clearly gleaned from the fact that not even a sign notifying the public of the surveillance activities taking place on the street was put up during the whole time of the project.

In the above-mentioned collaboration with the municipality, Het Nieuwe Instituut called for expanding awareness around data and the associated rights and duties. It referred to this as a social responsibility shared by the government, the market, research institutions, education, and cultural organisations (Vlassenrood, 2017, p. 17). Furthermore, it called for 'data transparency' from the side of both businesses and governments concerning the ways in which they handle data captured from the public sphere, not only to ensure that they are accountable, but also to facilitate critical examination of the impact of such data (*ibid*., p. 18). In an attempt to answer questions relating to which data are collected for Eindhoven municipality, for which purposes and how the public interest is understood in that context, the project set up the 'Embassy of Data' exhibition. In this exhibition they offered an installation visualising the types of data collected (including a special part dedicated to the *SLL*), alongside brief explanations of the actors, their purposes, and provocative questions, such as:

401 As with consensus, these techniques are often combined with other techniques of regulation, such as command. Such hybrid measures include mandatory disclosure of information in order to facilitate more informed decision-making by citizens.

402 See Eindhoven. (2017). Unity 3d model van Stratumseind. Retrieved March 31, 2019, from https://data.eindhoven.nl/explore/dataset/unity-3d-model-van-stratumseind/information/.

'Do you think that data can play a role in solving problems in society?'; 'Should others be able to sell your data?'; and 'Do you find your data valuable?'[403]

While this is a good beginning, relying too much on this type of regulatory tool in the case of surveillance of public space within smart cities and living labs, is not a good idea. Firstly, complete transparency concerning data analysis performed by businesses is not likely (or impossible) in view of trade secrets and intellectual property rights. A further issue with disclosure-based schemes is that they assume that citizens are rational decision-makers and are capable of accurately understanding and evaluating the data provided, which is not always the case. Various empirical studies have indicated that the impact of information on individual behaviour is highly context-sensitive and that individuals behave in complex, contingent and sometimes unpredictable ways in response to risk (Morgan & Yeung, 2007, pp. 97–99).

In the context of surveillance in public space, disclosure is a particularly problematic tool of regulation, since it might be taken to imply that with clear notification of surveillance, all problems are solved. This is based on the idea that persons can (and should) adapt their behaviour in accordance with the notified surveillance (e.g. one should not shout obscenities, unless they want to be caught on the sound sensors and subsequently by other technologies and potential humans in the loop). Yet, persons often do not behave in a (completely) rational way, especially when they are intoxicated, which is very common on a nightlife street such as Stratumseind. Moreover, in cases where complex algorithms are used, it is difficult to understand and explain the workings and decisions of the models (see e.g. Edwards & Veale, 2017). Also, while one might rationally find such surveillance acceptable for the purpose of safety, this is not necessarily so for other purposes, particularly regarding private purposes like increasing profit for businesses. In such a case, a well-notified person would still have the possibility to avoid the Stratumseind street. However, this would not be a very good option in the case where most of their friends would still want to visit the street. Furthermore, this approach might also amount to a spread of surveillance technologies in public space ('since all it takes is clear notification'), potentially leading to an increasingly surveilled city, in which one would have little (or no) choice of avoiding such places and being unobserved and 'un-nudged' by sensors and actuators in public space.

403 Original in Dutch: 'Denkt u dat data een rol kunnen spelen om problemen in de samenleving op te lossen?'; 'Vindt u uw data waardevol?' (translation by author).

4.1.2 Command: limits and possibilities

The law clearly has its limits, especially when it comes to regulation of complex and disruptive technological developments (just think of Airbnb and cryptocurrencies). Nevertheless, it still has an important role to play, especially, if we think of the law as one of the tools of regulation alongside others, including its role of laying ground rules for other regulatory tools (particularly consensus and communication).

Regarding surveillance in public space, several strands or bodies of law are relevant, in particular data protection law, human rights law, criminal (procedure) law, and administrative law. I will briefly discuss these and their suitability for regulating surveillance within smart cities below.

At the moment, it seems that data protection is leading the way in regulating the functioning of smart cities, living labs and similar data-based initiatives. This is certainly a good thing and data protection law has led to several notable limitations in regard to data processing, also in public space. It is likely to lead to more profound changes in view of the General Data Protection Regulation (GDPR). For instance, data protection law seems have put a stop (at least, temporarily) to the use of cameras in digital billboards in the Netherlands, the intention of which was to profile passers-by and serve them personalised advertisements. According to the Dutch Data Protection Authority (DPA; *Autoriteit Persoonsgegevens*), this amounts to personal data processing (even in the case of blurred images), so that *explicit* consent (for example, in the form of tapping yes to a request for personalised advertisements via an app on one's phone) is needed as a legal basis; without such consent video surveillance is not allowed.[404] The GDPR also requires an obligatory data protection impact assessment for data processing that 'is likely to result in a high risk to the rights and freedoms of natural persons' (Article 35 GDPR), as can be said about widespread surveillance in public space in the *SLL* example.

However, there are certain issues with and limitations of data protection law in regard to regulation of surveillance within such initiatives.[405] Firstly, it is very much unclear which regime would be applicable in cases of PPPs, such as the *SLL* – the GDPR or the

404 See Autoriteit Persoonsgegevens. (2018). AP informeert branche over norm camera's in reclamezuilen. Retrieved March 27, 2019, from https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera's-reclamezuilen#subtopic-1727.

405 I explore the topic of data protection law as a means of regulation of surveillance in the context of smart cities and living labs (taking the *SLL* as an example) in more detail in a separate paper co-authored with Raphaël Gellert, provisionally called: 'Regulating smart cities and living labs: an impasse for data protection? A discussion of the *Stratumseind Living Lab*'.

Law Enforcement Directive.[406] These regimes lead to rather different obligations. Data protection law still seems to make a very clear and strict distinction as to the goals of personal data processing, even when such processing is taking place within public-private partnerships where the means, tasks, goals and responsibilities are everything but clear and distinct. When the processing is performed by private parties and the goal of the processing is to secure private goods or persons or another commercial interest, the GDPR applies; when the processing is performed by a public actor and the goal is a task concerning the safeguarding of public security (or in connection to the prevention, investigation, detection or prosecution of criminal offences), the Law Enforcement Directive (and national laws based on this Directive) applies. Such an artificial distinction when discussing the regulation of camera surveillance within public-private partnerships can still be found in the 2016 Policy rules on camera surveillance in public space of the Dutch DPA.[407]

In the example of the *SLL*, such a strict distinction seems impossible: the technology (both hardware and software) is developed and provided by private parties (with some input from the municipality and the police); the actual surveillance is performed by the technology itself and representatives of the municipality (the police is only notified, when a disturbance is detected); and commercial goals are inseparable from the maintenance of the public order and safety part of the goals and they are attempted to be achieved through the same means and actors.

Furthermore, there are additional issues with data protection law, as pointed out by several scholars (e.g. Hildebrandt & Koops, 2010; Koops, 2014). These include issues pertaining to the data minimisation principle, pseudonymisation, consent, and enforcement, which go beyond the scope of this Section.[408] For instance, sticking to preconceived notions of what the purpose of a specific data mining operation will be is in direct opposition to the paradigm of 'big data'. Moreover, as seen in Chapter 5, the use of inferred profiles does not depend on personal data, rather, profiles are often

406 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

407 See Autoriteit Persoonsgegevens. (2016). Cameratoezicht - Beleidsregels. Retrieved from https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

408 These limitations of data protection law in the context of smart city regulation are planned to be examined in a future co-written paper.

inferred from anonymous or pseudonymous data and do not refer to any particular person. It will suffice here to state that the regulation of surveillance within smart cities and living labs needs to go beyond data protection law.

The human right to respect for private life in Article 8 ECHR also plays an important role in this context. As can be seen from the analysis in the previous Chapter, perhaps somewhat surprisingly, Article 8 offers a rather substantial protection of individual's privacy in public spaces. The Court has made clear that the place of intrusion is not a key factor in determining, whether an intrusion has occurred or not. Instead, the Court places more importance on the type of activity (private or public, dependent on several factors) and, especially, on the question, whether data relating to private life of an individual was stored or processed. Particularly pertinent for surveillance in public space is the Court's establishment of the right to lead a private social life, which 'may include professional activities or *activities taking place in a public context*',[409] recognising that the role of privacy includes the formation of social relations, also in a public context. Notably, Article 8 also protects individuals both from government activity as well as government inactivity in relation to intrusions by private actors. The Court's case law makes clear that even relatively minor interferences with Article 8 (among which it considers video surveillance in public space) must adhere to the general principles against arbitrary interference. Nevertheless, the human right to respect for private life still conceives privacy as solely an individual right and with limited value for society and democracy. Moreover, Article 8 case law seems to suggest a rather stringent requirement of data relating to an identified individual that has been harmed or is at risk of being harmed due to data processing based on a factual, case-specific assessment. As such, its protection in relation to the surveillance within the *SLL*, where persons are surveilled and affected as a part of a group, might be limited (although the Court's evolutive approach to the rights and freedoms shows a certain willingness to adapt the protection to new challenges, particularly in view of *in abstracto* claims).

However, human rights law (as primary law) generally sets standards that should be incorporated into secondary, particularly statutory law. Without such secondary law regulations, effective and timely protection of privacy in public space is difficult to achieve. One may lodge a complaint against a state before the ECtHR, however, before can do that, one needs to exhaust all national legal remedies (although some exceptions are possible), which is clearly burdensome. It also takes several years

409 National Federation of Sportspersons' Associations and Unions [FNASS] and others v. France (2018), Applications nos. nos. 48151/11 and 77769/13, § 153 (emphasis added).

between lodging a case to the ECtHR and, if the case is not manifestly ill-founded, a judgment.[410] It is thus a time-consuming procedure, not allowing for quick solutions. This is, of course, appropriate for such an institution.

In this context, criminal procedure law is of value. It regulates surveillance activities as used by law enforcement for purposes of criminal investigation and crime prevention, typically with substantial safeguards in place (e.g. Koops, 2016, 2016). However, this is generally not the case in the *SLL* example. In the *SLL*, one of the main purposes of surveillance is to enhance safety and to preserve public order, particularly by detecting or preventing 'escalated' (deviant or anti-social) behaviour, which is not necessarily or even primarily criminal activity. As such, surveillance does not focus on suspects but on all citizens and many forms of non-criminal behaviour are discouraged in such space (or suppressed, if more coercive measures are used). The Dutch police have referred to this as 'innovative non-criminal enforcement strategies' (NPI 2005; as quoted in Koops, 2009, p. 113).[411] Moreover, this is being done by both public and private actors (businesses). As such, criminal procedure law does not play a key role here and cannot be seen as the main type of law to regulate smart city/living lab surveillance. Instead, the body of law that would be much better suited to regulate it is administrative law,[412] which is arguably in need of an update.

Of course, by suggesting an update of legal protection in this context, I do not mean to say that we should throw away the baby along with the bathwater. Data protection law, protection of privacy in criminal procedural law and the human right to respect for private life should continue playing their role and remain very important in

410 The Court examines applications in a certain order, which takes into account the importance and the urgency of the issues involved. This means, for example, that the most serious cases or those which reveal the existence of problems on a large scale will be given priority. In 2017, 25% of leading cases pending before the Committee had been pending for 2-5 years, as compared to 29% in 2016. See Moxham, L. (2018). Implementation of ECtHR judgments – What do the latest statistics tell us? Retrieved from https://strasbourgobservers.com/2018/07/27/implementation-of-ecthr-judgments-what-do-the-latest-statistics-tell-us/.

411 The 2005 strategic vision of 'information-led investigation' of the Dutch Council of Chiefs of Police stated: 'the police have applied a large number of innovative non-criminal enforcement strategies, varying from regular control actions (police control) of infrastructural junctions in big cities, specific controls of hotspots and target groups (nightlife)' (as quoted in Koops, 2009, p. 113).

412 In general, administrative law deals with the decisions and activities of public institutions and, in particular, specifies the means of challenging their validity and providing remedies for grievances (Morgan & Yeung, 2007, p. 137). As with most laws, there are significant differences between countries regarding the character and effectiveness of administrative law. In this Section, I will discuss possible measures only in the abstract, so these I will not discuss these issues further.

protecting privacy. Rather, what I am proposing is that these should be supplemented with additional forms of legal protection that fill in the emerging gap in protection of citizens against smart city and living lab surveillance.

The idea that this important role should fall on administrative law is not particularly new (e.g. Koops, 2009). As Koops put it:

> 'When crime control shifts from criminal investigation of committed crimes to criminal risk governance, the cornerstone of legal protection is no longer the judge who checks power abuse in court or during criminal investigation, but the accountant who audits the correct, fair, and transparent functioning of the law-enforcement system at large' (Koops, 2009, pp. 121–122; referring to van Swaaningen 2004).

The types of protection mechanisms needed are administrative and accountancy-type checks and balances, such as reporting and complaint mechanisms, internal auditing, ombudswomen, special councils, public participation, a focus on decisions that affect people's lives, as well as adequate funds and powers (Koops, 2009; Slobogin, 2016, 2018). Such supervisory bodies are said to be better suited than criminal courts (or human rights courts) to check the power imbalances inherent to the new 'public order'. According to Koops (2009, p. 122), they also allow for more flexibility in calling 'criminal risk managers' to accountability, since these may be business managers or bureaucrats of public-private partnerships as soon as traditional police officers. Of course, such mechanisms already exist to some extent, but in their current forms, they are peripheral rather than core procedures, in need of substantial increase in powers and resources to become really effective.

Although some scholars remain doubtful of the capacity of administrative rules to protect citizens from smart environments (e.g. Hildebrandt, 2011; Hildebrandt & Koops, 2010), these types of mechanisms might nevertheless be best suited (at least, among the strands of law mentioned above) to address the types of privacy-related risks, which stem from PPPs, and have a broader societal impact. There is a need for such legislation, particularly in the Netherlands, where only *video* surveillance is specifically regulated in the Municipality Act (Gemeentewet; Art. 151c)[413] and the local

413 See Gemeentewet. (n.d.). Retrieved March 31, 2019, from https://wetten.overheid.nl/BWBR0005416/2019-01-01.

ordinances (Art. 2:77 Municipal ordinance Eindhoven [*Algemene Plaatselijke Verordering Eindhoven*]).[414]

Particularly in the U.S., legislative development through administrative law has recently been at the fore, largely as a reaction to concerns about privacy and a lack of transparent and accountable processes of acquisition and use of surveillance technologies by the police and the significant gaps in federal and state privacy laws (Rubinstein, 2018). Several cities and counties (including, Santa Clara County, Berkeley, Seattle, Oakland, New York City) have enacted local ordinances (laws enacted by a municipality or other local authority), a type of administrative law, regulating the acquisition and use of surveillance technologies, irrespective of whether they monitor private or public space. While these legal instruments in the U.S. generally apply to law enforcement, they may also apply in cases when surveillance technology is used within PPPs (e.g. Seattle Surveillance Ordinance 125376).[415] These legal instruments are seen as fundamental to minimising the risks posed by the use of such technologies by law enforcement, especially in relation to privacy, freedom of speech, freedom of association and a disparate impact on particular groups (Rubinstein, 2018, pp. 2038–2039). In particular, these ordinances establish internal and external oversight, including auditing, privacy city councils (the approval of which prior to the acquisition and use may be required), chief privacy officers[416] and data governance policies. They also require surveillance impact assessments (SIAs) and that protocols disclosing intended use and deployment of surveillance technologies (including information about data collection, use, access, retention, and sharing with other entities), are prepared and published (*ibid.*).[417]

Clearly, the ordinances share many similarities with European data protection law (and, as such, they share their problems) but they also go beyond them. Particularly

414 See Gemeente Eindhoven. (2018). Algemene Plaatselijke Verordening - Eindhoven. Retrieved March 31, 2019, from http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Eindhoven/415534/415534_2.html.

415 See the City of Seattle's Surveillance Ordinance 125376. (2017). Retrieved March 31, 2091, from https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance.

416 In the Seattle Surveillance Ordinance, for example, this body has the authority to order any department that is out of compliance to cease acquisition or use of the surveillance technology (Rubinstein, 2018).

417 See also: ACLU. (2018). Community Control Over Police Surveillance (CCOPS) Model Bill. Retrieved March 31, 2019, from https://www.aclu.org/other/community-control-over-police-surveillance-ccops-model-bill.

by establishing auditing procedures, privacy councils with power of approval and obligatory publication of relevant information (including the surveillance technologies acquired and for which purposes),[418] these requirements would ensure a higher level of control as well as increased citizen involvement in the decision-making of how to preserve the safety and livability of their cities. Moreover, with a broader focus on regulating power shifts between the municipality (or the state more broadly), businesses and citizens, their approach could go beyond individual harm and risk, encompassing privacy-related risks for algorithmic groups within contemporary smart cities and living labs. In cases of secret surveillance measures for purposes of criminal investigation, revealing information about surveillance can defeat its purpose (and is accordingly regulated in criminal procedure laws). However, the same does not apply to the type of surveillance found in the *SLL* and similar initiatives, where surveillance is deployed more or less continuously regardless of crimes or misdemeanours being committed and targeting no one in particular.

Similar provisions could be envisioned for the Dutch municipal ordinances (APV) or other similar legal instruments, which for the time being lack any specific regulation of surveillance other than video surveillance (e.g. Eindhoven APV). Based on the analysis of ECtHR case law in Chapter 6, a clear legal basis and safeguards in the law are required even for relatively minor intrusion into persons' privacy in public space, let alone for a more extensive type of surveillance occurring on the Stratumseind street.

Furthermore, in view of the privatisation and securitisation of public space and the implications of this for our public and private lives, regulators should take notice of the fluid and overlapping boundary between public and private spaces. If cities are becoming riddled with privately owned and managed public spaces, such as corporate parks and squares, where access and activities are tightly regulated in line with private interests, the law should make it clearer that liberties connected to public space, such as the right to representation, assembly and freedom of action in urban open spaces, are protected in these new types of public space as well.

4.1.3 Code: from software to physical architecture

Code- or architecture-based techniques operate in direct contrast to communication-based techniques, which appeal to rational reasoning. Instead, regulation through code ('techno-regulation') seeks to eliminate undesirable behaviour by designing

418 E.g. Seattle. (2017). Master list of surveillance technologies. Retrieved March 31, 2019, from https://www.seattle.gov/Documents/Departments/SeattleIT/Master-List-Surveillance-Technologies.pdf.

out the possibility of its occurrence (Morgan & Yeung, 2007, p. 102). According to Brownsword (2005), techno-regulation functions in such a way that those regulated have no choice but to act in accordance with the desired regulatory pattern, rather than only making certain actions more difficult. For example, making it impossible to enter or exit a train station without a valid ticket, as has become common in the Netherlands (although one can still jump the rails, stretch over them to 'chip in' and then 'chip out' again or exit closely behind another person). Techno-regulation in this strict sense, it seems, is much more suited for the online environment (for instance, by only offering pre-determined options to choose from), where the 'computer says no' has been a well-known trope for decades.

A similar type of regulation can be seen in the *SLL*, where possibilities for de-escalating behaviour are attempted to be designed into the environment itself (through light and smell scenarios). As such, they do not really make it impossible for persons to behave in an escalated manner, rather they try to make it more difficult. As mentioned above, the *SLL* may thus be seen as a hybrid regulatory tool (combining competition, consensus and code tools), trying to regulate persons' behaviour through code for purposes of profit and safety.

Another way of looking at code or architecture as a regulatory tool would be to think of designing *in* opportunities for achieving privacy in public space.

The experience of privacy is closely tied to space and its use, which has been confirmed by experiments in studies of crowding (e.g. Gillis, 1979; Gove & Hughes, 1980). Architectural elements (working together with behavioural mechanisms, particularly civil inattention and reserve) have been acting as regulators of privacy in both private and public space for ages. Doors, locks, windows, curtains and furniture have provided persons ample opportunity both to be let alone as well as to interact with others. Similarly, hedges, walls, narrow alleys and tunnels have provided such opportunities in public space. In contemporary public space, enhanced with a layer of sensors that can 'see' and 'hear' far away and in close-up,[419] some even through walls and in the dark,[420] such opportunities are considerably limited. While setting limitations to the use of such surveillance technologies in public space in law is certainly desirable (as discussed in the previous sub-section), another line of thinking would be to design

419 Think of video cameras embedded with facial recognition capability, drones equipped with video and sound sensors and infrared cameras.

420 At least in the sense of detecting heat through walls.

opportunities for privacy in the physical architecture and, especially, in the code of public space itself.

The idea behind this suggestion is that environments should be supportive of users' privacy needs and (to a certain extent) desires, facilitating the behavioural processes used to regulate interaction (Witte, 2003, p. 8). This idea stems from Altman's theory on privacy as a boundary marking process, according to which people seek a balance between closedness and openness in relation to others (Altman, 1976; see Chapter 3), which is also broadly in line with the above conceptualisation of privacy *for* public space. Following Altman's theory, an environment needs to be supportive of persons' dynamic regulation of privacy, rather than only promoting either social interaction or solitude. This is, of course, not an easy task, as the desired level of privacy[421] is dynamic and varying so that it cannot be abstractly predetermined. Architecturally then, 'the environment must respond to the user's desire, by allowing [her] to take control over the environment' (Witte, 2003, p. 32). According to Witte (*ibid*., p. 64) such an environment should thus have several characteristics, such as: (1) allowing for easy alteration between areas of separation and togetherness; (2) responding to persons' desires for openness or closedness; (3) allowing for a continuum of privacy levels; (4) permitting different degrees of control depending on possession; (5) allowing for personal space; and (6) creating clearly defined territories.

Since open public space is traditionally considered common space, in which no person or group of persons have the right to claim control over the place and exclude others, architectural regulation of privacy following this perspective is more limited than in regard to enclosed public space (e.g. libraries) or private space. Nevertheless, these characteristics still offer a good foundation to think of an open public space that would be conducive both for being alone and interacting with others.

The first lesson that one can take away is that public space should allow for places that are not covered by surveillance technologies. This means that even if the Stratumseind street is surveilled as it is now (if sufficient justification and safeguards are in place in line with the law), nearby streets should offer opportunities of hiddenness, both for snogging one's girlfriend (interaction) as well as for shedding a tear (being let alone). Surveillance of public space should thus not creep into every corner of the city (or

421 Altman (1975) distinguishes between a 'desired' and an 'achieved' level of privacy. Desired privacy is a 'subjective statement of an ideal level of interaction with others' (*ibid*., p. 10). Achieved privacy is the 'actual degree of contact that results from interaction with others' (*ibid*.). When these are equal, an ideal level of privacy exists.

the village) so as to leave little or no space of remaining unobserved. In this sense, Solove's (2007, p. 747) requirement of preserving 'free zones' in order to give persons the possibility to present themselves and be present in public for various purposes, can be taken quite literally in the sense of preserving networked surveillance-free zones in the physical spaces of smart cities (as a sort of counter-part to the existing 'security zones'; see Chapter 4). The 'traditional' understanding of privacy rights protecting 'people [that is, individuals] not places' (this idea originated in the Katz v. United States judgment but has also been employed in the case law of other countries; see e.g. Reiter, 2009), might thus be *complemented* with the opposite approach – that is, protecting places in order to protect persons.

The second lesson concerns the clear demarcation of territories. While an obligation to notify persons of CCTV in a clear and visible manner at the place of observation has been in place for a long time, there is as yet no such obligation for other types of surveillance activities (except for the general right of the data subject to be informed in Article 13 GDPR). The purpose of notification of surveillance relates to the fact that persons need to be able to determine the context in order to adapt their behaviour accordingly. However, in relation to 'smart environments' (Hildebrandt, 2011, p. 226) that are capable of anticipating human behaviour and reacting to it accordingly (e.g. in order to offer personalised advertisements or a calming lighting scenario), such adaptation is difficult if not impossible (I have discussed issues with autonomy in Chapter 5). In smart environments, 'a clear demarcation of territories' is therefore not a good option.

What might be more suitable and desirable for such a smart environment would be to implement some administrative law checks and balances and data-protection-by-design features (particularly data minimisation and purpose specification) (Edwards, 2016). Of course, more innovative approaches to regulating smart environments are also desired (e.g. Hildebrandt, 2008a envisioning 'Ambient law', that is, 'legal protection by design', 2011), however these are as yet underdeveloped, so that it is difficult to propose any more concrete suggestions for implementation.

While one cannot determine each person's desires or needs for privacy, one can broadly differentiate between different contexts in relation to the *SLL*, including nightlife, daytime and political activity, which generally require different levels or types of surveillance. These distinctions could, to a certain extent at least, be inscribed within the *SLL* technological system itself. This is generally in line with Altman's privacy as boundary management theory, according to which when a physical space changes (for instance, it becomes surveilled via various types of technologies), a person's ideal

degree of disclosure does not necessarily change with it. Instead, people will cope with this change by using other, often behavioural mechanisms in order to preserve a similar degree of disclosure (e.g. saying less, lying, not associating with certain persons or not participating in an event) (Kaminski, 2015, p. 1116). As I have concluded in the previous sub-section when discussing administrative checks and balances, the government thus has an interest in preserving some situations as surveillance-free or surveillance-limited to prevent undesirable behavioural shifts, either because particular activities are so valuable (political participation) or because they could have other significant consequences (*ibid*., p. 1136).

For instance, during the daytime and in the absence of any concrete risks, when the street would be rather empty, the system should be capturing and analysing very little (or no) data from the passers-by or visitors of the street, as there would be no justification for broader capture or analysis. Administrative law could and should specify certain conditions and justifications according to which surveillance of daily life in public space beyond CCTV could take place. In the case of a political protest discerned through the data capture (or otherwise), the *SLL* system should limit data capture, analysis and enforcement (that is, action taken based on the analysis) capabilities to the purpose of preservation of safety. This goal should, however, not be interpreted too broadly, as offering a *carte blanche* for surveillance. As long as the protest is peaceful, nudging tools (and certainly coercive tools) should not be used (or should be used with serious reservations, perhaps with a higher-ranking police officer in the loop).[422] No nudging or capture of data for other purposes (e.g. increasing consumption) should be used.

In contrast, in the nightlife context (e.g. on a Friday evening), when risks for safety would be higher, the *SLL* system could be more alert, that is capturing more types of data and analysing them for the purpose of preserving the safety. Nevertheless, even within such a context, a certain level of 'indeterminacy' (or 'uncertainty') in relation to the outcome of the analysis (or regarding enforcement) within the automated system might need be preserved. This indeterminacy refers to the fact that the data provided by a set of sensors might be incomplete, so that automated decisions based on such data might be inaccurate, invalid or otherwise undesired (Hartzog, Conti, Nelson, & Shay, 2015, p. 1785). In this sense, Hartzog et al. (*ibid*.) propose to design a level of 'indeterminacy' into the automated systems. This means that the system would leave in the possibility of choice (depending on context), requiring a level of interpretation by a human in the loop. Although these scholars are referring

422 Precisely how this would be implemented in the technology goes beyond the scope of this section.

specifically to automated law enforcement, a similar argument can be made in regard to 'innovative non-criminal enforcement strategies', as the Dutch police put it. Such indeterminacy (and thus a human in the loop) would not be needed in every case, but would be desirable in cases, when a higher level of risk would be determined by the system, calling for more intrusive measures (e.g. putting persons on a list of troublemakers, use of the 'Mosquito', exclusion).

5. FINAL CONCLUSION: SUMMARY OF FINDINGS AND ANSWERS TO THE RESEARCH QUESTIONS

In this dissertation, I have explored the issue of privacy in public spaces within the context of surveillance in smart cities and living labs. I have done so not only through a theoretical perspective but also by examining an example of a living lab in practice – the *Stratumseind Living Lab* (*SLL*) in Eindhoven, the Netherlands. Drawing from four different fields of research (human geography, surveillance studies, privacy theory and law), I have combined concepts and developed a heuristic that can help us think about and regulate privacy in the changing context of contemporary public spaces, particularly in Europe.

The focus of this dissertation thus arose out of the context of contemporary transformations of cities into smart cities and – connected to this – living labs. This is something that can be observed globally but that takes on particular characteristics in historical city centres of European cities, bigger and newer cities in the U.S. or in South Korea. As the practical example of the *SLL* is situated in a continental European legal system, I have focused my research on smart city developments in continental Europe, particularly the Netherlands. A key part of these transformations is the widespread and pervasive surveillance of public space, through the introduction of sensors, actuators and other types of surveillance technologies, such as smart video and sound cameras, wifi tracking and various types of nudging technologies. Achieving privacy in public space is, therefore, becoming increasingly difficult. And while the notion of privacy in public is becoming less and less contentious in privacy and legal theory, it is still underdeveloped. The question how we should think of and regulate privacy in public space in this context is, thus, a pressing question in privacy and legal scholarship.

While several privacy scholars have discussed the notion of privacy in public space particularly since the end of the 1990s (most notably Koops, 2018; Nissenbaum, 1997, 1998; Paton-Simpson, 2000; Reidenberg, 2014; Rubinstein, 2018; Sloan & Warner,

2015; Slobogin, 2002), they have mostly done so in a piecemeal manner in a paper or two.[423] And despite recent edited volumes on the topic (e.g. Newell et al., 2019; e.g. Timan, Newell, et al., 2017b), a thorough conceptual examination of the topic is still missing. As such, privacy in public space may still be described as somewhat of a neglected topic. In this context, I have attempted a thoroughly interdisciplinary analysis of this concept in the dissertation. Instead of examining the concept solely through established perspectives in privacy and legal theory, I have broadened the scope by including the view of surveillance studies and human geography. This has allowed me to better analyse particular surveillance practices in living labs (using both the example of the *SLL* and short hypothetical scenarios, enabling me to go beyond the particular successes and failures of the example) and the types of risks related to privacy that they pose. This led me to pose the following main research question and sub-questions:

How can and should we conceptualise privacy in public space, especially within the context of surveillance in smart cities and living labs?

(1) *How should we think of smart city and living lab initiatives (at least those in the West) and what challenges do they pose, especially in relation to privacy?*
(2) *How does the practical example of a living lab in the Netherlands – the Stratumseind Living Lab (SLL) – inform these theoretical insights?*
(3) *How is surveillance conceptualised in prominent literature, particularly in surveillance studies?*
(4) *How is privacy – both as a concept and as a set of legal rights – conceptualised in general, especially in Europe?*
(5) *How is public space conceptualised in prominent literature (primarily in urban geography and political theory) and what are the key interests and rights connected to public space?*
(6) *What types and characteristics of surveillance can be discerned from the SLL example and what kinds of privacy-related risks do they pose?*
(7) *Does the right to respect for private life in Article 8 of the European Convention on Human Rights (ECHR) protect privacy in public and, if so, based on what reasoning and to what extent?*

The sub-questions represented thematic-chronological steps in the process of answering the main question, which finally led me to conceptualise privacy *for* public space (PfP). In the concluding Chapter I have furthermore tried to open up the debate based on this rough outline of a conceptualisation by briefly examining possible tools

423 A notable exception is Nissenbaum, who dealt with the topic in a more extensive manner (see 2010).

for regulation of surveillance within living labs and smart cities in order to address the various types of privacy-related risks stemming from it.

In the next paragraphs, I provide a brief summary of the main research findings, coupled with the research question and sub-questions. I have structured the dissertation in two general parts: in the first part, I examined the 'foundational notions' of this dissertation: smart cities and living labs, surveillance, privacy and public space (Chapters 1-4). In the second part, I brought these notions together by analysing their articulation in two particular contexts: in Chapter 5, I connect surveillance and privacy theory to the *SLL* example and, in Chapter 6, I analyse the right to respect of private life in Article 8 ECHR as it applies to public space, activities and data. The dissertation can, thus, be described as kaleidoscopic – each chapter provides a somewhat different perspective on the same matter: privacy in public space in contemporary living labs and smart cities.

In the first Chapter of this dissertation, I offered a general discussion of smart cities, living labs and the example of the *Stratumseind Living Lab* (*SLL*). I began the discussion in this way in order to offer an illustrative example to which one can apply the abstract notions of privacy, surveillance and public space that follow. In this Chapter, I have answered the first two sub-questions. I determined that the term smart city generally refers to the practice of extensive embedding of software-enabled technologies (particularly ICTs) into the city environment for two broad purposes: augmenting urban management and improving the quality of life in the city and stimulating the economic development of the city. In this age, 'city space is both an economic and cultural resource that melts into one' (Roberts, 2008, p. 664). Living labs are initiatives commonly connected to smart cities. They refer to an experimentation environment and methodology for organising multi-stakeholder innovation processes, including users and communities of users, in a real-life setting, and aimed at the exploration, co-creation and evaluation of innovations. Connecting the notions of smart cities and living labs, I have observed that the deployment of living labs is said to represent a bottom-up approach to the smart city, designed to increase citizens' participation and involvement in solving social issues.

A detailed examination of the *SLL* example (particularly three sub-projects: *CityPulse*, *De-escalate* and *Trillion*; complemented with research into living labs in the Netherlands done by the Rathenau Instituut; 2017), however, painted a different picture. This living lab with a focus on both safety and profitability did not represent an actual bottom-up approach to the smart city. Quite the opposite, it offered a practical insight into the common critiques of such initiatives found in urban geography literature: ideological

rhetoric, a technocratic form of city governance and a neoliberal ethos. When thinking about smart cities and living labs, one thus needs to go beyond the grand promises of such projects and examine them both in their concrete practices and contexts as well as through other perspectives, including surveillance and privacy theory. In order to thoroughly analyse privacy-related risks stemming from surveillance within such initiatives, including possibilities for its regulation, insights from these various fields need to be brought together, possibly leading to a sum that is more than its parts.

This discussion was followed by a chapter on surveillance theory, offering a very different perspective on the innovative projects calling themselves living labs and smart cities. In Chapter 2, I proposed a rough chronological-thematic overview of surveillance concepts and theories in the form of three phases, thus answering the third research sub-question: *How is surveillance conceptualised in prominent literature, particularly in surveillance studies?*

The first phase, featuring Bentham and Foucault, revolves around the Panopticon and panopticism, and can be described as offering architectural theories of surveillance. The second phase moves away from panoptic metaphors and shifts the focus from institutions to networks and to relatively opaque forms of control. This phase can be characterised as offering infrastructural theories of surveillance and includes Deleuze's notion of control societies, Haggerty and Ericson's surveillant assemblage and Foucault's notion of security. In the third phase, we find surveillance theory building on, and sometimes combining insights from, both theoretical frameworks of the first two phases, to conceptualise surveillance through concepts or lenses of dataveillance, access control, social sorting, peer-to-peer surveillance and resistance.

The main aim of this Chapter was to provide a more structured insight into the various forms of surveillance and to show that choosing a surveillance framework through which to analyse a particular type and context of monitoring matters. An analysis of surveillance within the *SLL* through the lens of the prison Panopticon (as is still very common) or Foucault's security will shed different lights on the matter and thus lead to different implications for human rights. The analysis in this Chapter has helped me to identify the general characteristics of the three surveillance phases, through which I have analysed the surveillance taking place in the *SLL* example in Chapter 5. I have done so by answering the following questions: the first, concerning the general characteristics of surveillance (physical, confined and stable, or numerical, networked, open and liquid), the second concerning the main actors of surveillance (the state, corporations and/or individuals themselves), the third in regard to the object of surveillance (the underclass, the productive citizen, individuals or groups,

the individual physical body or dividuals and data doubles), the fourth about the aim of surveillance (disciple, control and/or anything else) and, finally, the question relating to the perception of surveillance (sinister, beneficial or even entertaining).

Another key insight from this Chapter is that the various types and techniques of surveillance (and the three stages) represent modes of power that continue to exist alongside each other, rather than succeeding each other. Instead, in particular times and contexts one of these modes of power may come to be the dominant operational logic.

In Chapter 3, I offered a broad overview of the conceptualisations of privacy, both as a theoretical and legal concept. In this Chapter, I answered the fourth research sub-question: *How is privacy – both as a concept and as a set of legal rights – conceptualised in general, especially in Europe?* As I have explained in the Introduction, I have avoided a focus on the dominating type of informational privacy (and data protection law, especially in view of the GDPR), in order to shed light on other – just as pressing – aspects of privacy, discussed to a much lesser degree nowadays. The main aim of this Chapter was to make sense of this complex notion by breaking it down into more manageable pieces that might offer additional insight in this broken-down form. In particular, I examined the main underlying values of privacy (*why* we value privacy), the types and dimensions of privacy (specifying *what* is of value in privacy), and the mechanisms for achieving privacy (showing *how* privacy is achieved). I also addressed, at least partially, the question *whom* privacy protects, by giving reasons for valuing privacy for the individual as well as for society in general (which I do in the part on the value of privacy). Moreover, as the main focus of this dissertation is on privacy *in* public space, a part of the *where* aspect is found throughout the dissertation.

In the second part of Chapter 3, I also examined the main conceptualisations of the rights to (or the law of) privacy. One of the main insights of this Chapter for the dissertation was that privacy as a theoretical and linguistic concept has been evolving, both in the sense of changing in focus but also widening, ever since it emerged. And while several scholars consider the elusiveness of privacy as a problem, it can also be seen as a strength, the condition of its growth, particularly when responding to problems created by new technologies and societal change. This perspective is thus suitable for privacy in public space in the context of smart cities and living labs. If privacy in public did not exist as a practical problem in the recent past, simply because individuals achieved a generally satisfactory level of privacy there through social mechanisms, new practices and technologies of surveillance have changed this (Nissenbaum, 1998). Moreover, if a binary conception of private *versus* public (space,

activity or data) has served our privacy needs well enough until recently, this is no longer the case.

Another important insight stemming from the analysis in this Chapter is connected to the fact that privacy theory increasingly emphasises the value of privacy not only for the individual but for society and democracy more broadly. Moreover, privacy is seen not only as a value in itself but also as a value that is crucial in relation to other fundamental rights and freedoms, such as freedom of expression and freedom of assembly and association. Privacy is thus a 'part of a package of intertwined fundamental rights' (Gutwirth, 2002, p. 45) that guarantees not only our individual but also social and political emancipation. Or, as Koops (2018) put it, privacy is an infrastructural condition. It is an important presupposition for autonomy, self-development, and the other values that privacy contributes to; and it is because privacy can serve many other values that it is also a value in itself (ibid., p. 621). This is particularly valuable in regard to the relationship between surveillance and privacy, which is discussed in relation to the *Stratumseind Living Lab* in the Chapter 5. There is, namely, a particular disconnect between these two concepts. Surveillance studies scholars commonly employ a very narrow conception of privacy, often limited to a simplistic perception of the right to protection of personal data, positing that the risks of surveillance go much beyond risks for privacy. As such, their argument goes that privacy is not the sole or the best means to regulate surveillance (e.g. Lyon, 2001). However, in view of the infrastructural character of privacy (both as a concept as well as a right), this claim can and should be questioned.

Finally, the analysis in this Chapter enabled me to settle on a definition of the concept of privacy, which I employed throughout the rest of the dissertation. Following Julie Cohen (who nicely relates this definition to several accounts of privacy as described above; 2017, p. 458), I defined privacy as 'breathing room for socially situated subjects to engage in the processes of boundary management through which they define and redefine themselves as subjects.' As such, rights to privacy need to be understood in a similarly broad sense as 'the sociotechnical conditions that make condition of privacy possible' (*ibid.*). In other words, I concluded that privacy law needs to preserve the possibilities of achieving privacy (similarly Austin, 2019). As the concept of privacy is not rooted or limited to private space, this applies to public space as well. Indeed, a similarly broad conception of privacy (while not without its critics) seems to be found in the interpretation of Article 8 by the ECtHR, which I examined in Chapter 6.

In Chapter 4, I examined the last foundational notion, which is commonly overlooked in discussions about privacy – public space. The general aim of this Chapter was to

unveil various aspects of urban public space that are particularly relevant for the discussion and subsequent conceptualisation of privacy in public space. As such, I answered the fifth sub-question: *How is public space conceptualised in prominent literature (primarily in urban geography and political theory) and what are the key interests and rights connected to public space?* The central focus of this Chapter was on physical urban space of Western societies, with its particular political, social and psychological significance. As Kaminski (2015, p. 1114) put it, '[w]hile a growing number of scholars have discussed the importance of context to surveillance online, [surveillance] often gets neglected in the physical world.' As such, I examined public space from multiple perspectives. First, I employed a socio-spatial perspective, asking questions such as 'what are public space and place?' or, rather, 'how are public space and place made?' I then examined public space from a political perspective, engaging with theory on public and private spheres and, moreover, on the public-private distinction. In the third section, I analysed contemporary power shifts in public space, focusing on issues of privatisation and securitisation of public space. In connection to these issues of power, I briefly reviewed how law deals with public space, focusing on public nuisance laws and 'security zones'. Finally, in the last section, I delved into the connection between space and identity-building, especially in light of recent socio-technological developments such as time-space compression and de-territorialisation.

The first key insight stemming from this Chapter relates to the fact that public space is important for two general reasons: first, because it provides a physical space for interpersonal communication and social encounters that make a community possible (I have termed this 'sociability') and, second, because it represents the forum where – visible to others – individuals, groups, and crowds become political subjects. However, in relation to both of these functions, a special type of visibility is at play. In relation to political participation, Arendt's notion of the mask is important. Such a mask (today often referred to as anonymity) allows for a person's voice to be heard, while hiding individuals' (*idem*) identity in order to protect them from interference of powerful actors, both public and private, as well as peer pressure. Similarly, in order for public space to function as a space of sociability, encouraging mingling and interaction between strangers of various classes, races and ages, 'social distance' is needed. Such social distance is based on social norms and conventions (including civil inattention and reserve), which is connected to the transformation of public *space* into public *place*, an environment in which social trust exists or is at least possible. Without such trust, a community cannot emerge. Therefore, public space is not only a space of exposure, it is also a space of obscurity or inconspicuousness. However, in view of technological developments, these layers of obscurity and inconspicuousness in public space are at risk, thus endangering its two key functions.

The second key insight is that the public and the private exist in a complex and interrelated relationship. Unlike many legal and privacy scholars, geographers and political theorists have concluded a while back that public and private are inherently complex and unstable cultural categories that are mutually constructed. Therefore, the public sphere is not only a space of politics or sociability, it is also a space that is constituted in and through privacy. A person needs a time and space for herself (often at home, in her room), in order to develop her thoughts, opinions and identities before she can venture outside. Yet, if there is no public space into which one can venture and participate in the various activities of politics and sociability, an individual cannot fully develop into a citizen or community member and, thus, her personal development (her 'privacy') is limited as well. The public and the private (referring to spaces, activities etc.) are not binary oppositions; quite the opposite, they go hand in hand.

This is connected to the last insight, according to which public space is important for the construction of our identities, both individual and collective, providing a *locus* for identity. This is thus a function that public space shares with privacy (see Chapter 3). Identity, both individual and social (which are thoroughly interrelated), is nowadays conceptualised as a process (rather than as a fixed thing; see Jenkins, 2014). Not only is public space important to the construction of individual identity, especially in relation to becoming a fully-formed citizen, it is also important for the construction of group identities and communities. Social groups (as well as individuals), namely, do not exist *a priori*. In particular, it is the interactions that can and may occur in public space that are crucial for the formation of various social identities. As people build their identities in relation to places, particularly places where they feel at home or 'in place', identity and place construction need to be considered jointly as being co-produced. This suggests that privacy as the freedom (or breathing room) to define and re-define oneself as a subject (which is how I understand the concept of privacy; see Chapter 3) should be analysed in relation to place in all the richness, variation, and complexity that place entails, which goes far beyond a simplistic notion of a 'private place', epitomized by the home, that, in a legal and regulatory context, is still all too often associated with privacy. Identities connected to being-at-home of being-in-place are also constructed in public places, in movement, and in physical-digital networked spaces.

In the first chapter of the second part of the dissertation, I connected the insights gained from Chapters 2 and 3 and applied them to the *SLL* example. In particular, I used the example of the *Stratumseind Living Lab* (*SLL*) in order to determine the common types and characteristics of surveillance taking place in smart cities and living labs

focused on safety and profitability, at least in the West. This enabled me to answer the sixth sub-question of this dissertation: *What types and characteristics of surveillance can be discerned from the SLL example and what kinds of privacy-related risks do they pose?* I determined that the most prevalent surveillance techniques on the Stratumseind street are those from the second stage of surveillance theory. The primary logic is found in Foucauldian security (alongside the logics of Deleuze's notion of control, and Haggerty and Ericson's surveillant assemblage), where the focus is on the 'atmosphere' on the street and persons are governed as a multiplicity, rather than individuals. As such, the principle of such surveillance is inclusionary – smaller transgressions are overlooked as long as the atmosphere on the street (relating to relationships on the street as a whole) is not affected. So as to go beyond the particularities of the *SLL* example, I also employed short hypothetical scenarios, some more and others less speculative, in the discussion. These scenarios allowed me to identify and analyse several privacy-related risks stemming from the *SLL* but going beyond the particular successes or failures of the *SLL*.

The broad overview of surveillance types and characteristics enabled me to identify the particular risks related to privacy stemming from these surveillance practices. Notably, I spoke of 'privacy-related risks' rather than 'privacy risks'. This refers to my broad understanding of privacy (based on Chapter 3), which stretches from the development of identity and autonomy to the formation of social relations and requirements for democracy. As privacy also has an infrastructural character – it is of value on its own but it also contributes to other values, 'privacy-related risks' encompass broader risks stemming from surveillance, including social sorting, chilling effects and group profiling. The analysis in this Chapter has revealed several types of privacy-related risks stemming from the *SLL*, including: (re)stigmatisation, diminishing trust, profiling and the production of risk categories, disintegration and datafication of the self, exclusion, hindering social relations, risks for sociability, and narrowing down possibilities for autonomous (both personal and political) action as well as for the development and existence of multiple publics. While these risks are diverse, they can be structured in a few broad types of privacy-related risks. The most predominant privacy-related risks stemming from the surveillance within the SLL and similar initiatives are those that hinder:

(1) the development of identity (individual, social and political);
(2) the possibility of autonomous action (personal and political); and
(3) social interactions, both in relation to informal daily life as well as political activity occurring in public space.

There are several takeaways from this analysis. A general takeaway is that the risks concern both traditional privacy risks (that is, in relation to the individual), as well as risks relating to society and democracy more broadly, which have more recently been connected to privacy, as well as risks closely connected to the values of public space itself (especially seen in the third type). More specifically, the analysis has confirmed that a relatively new type of privacy risk is at the fore today – privacy risks concerning groups (most often, algorithmic groups based on profiling). In line with Foucault's theorisation of security, the focus of surveillant activity is on relationships between persons and the environment they are in, in order to affect the general atmosphere on the street, transforming it into an 'atmosphere conducive to consumption'. As such, individuals need not be individually identified, yet they may still be individually 'reachable', that is, subject to consequential inferences, predictions and nudges taken on that basis (Barocas & Nissenbaum, 2014). Another insight is that in the specific context of smart city and living labs surveillance in public space, the social and political value of privacy are at the forefront. I do not mean to say that the classical individual values are no longer implicated – they still are. However, the broader value of privacy as developed in the more recent accounts seems to be at particular risk through the new types of surveillant technologies and their manners of operation. Privacy in public space, namely, does not focus on disengaging the individual from social and political life, as follows from the traditional liberal perspective on privacy. Quite the opposite, privacy in public space focuses on facilitating the development of a broad range of social relations, including the aims of political association. Privacy thus has a strong facilitative role here (exhibiting its infrastructural nature), as privacy in public space allows for a more secure and fuller exercise of other rights and freedoms, in particular freedoms of assembly and association, of expression, and of movement.

This is connected to the insight based on Chapter 4, according to which surveillance within smart city/living lab initiatives also shapes the texture of public places in functionally specific ways that may be detrimental to both political and informal community life. It does this particularly by valancing multiple-purpose public spaces for particular patterns of use (Patton, 2000, p. 186). Surveillance of public space within the *SLL* creates an environment that is conducive to consumption (in this case, consumption in the pubs on the Stratumseind street). This orientation towards consumerism (which also excludes potential sources of nuisance) is neither conducive to encounters and debate nor to political participation (Lofland, 1998). This means that key functionalities of public space, sociability and political participation, are hindered. In this sense, Patton (2000, p. 181) asked, what is at stake besides privacy when it comes to surveillance of public space. 'How does protecting privacy in public places fail to address the social and cultural significance of public places? People do

not value public places for protecting privacy. Rather, public places provide a basis for informal sociality and civic life' (Patton, 2000, p. 181). Patton was onto something. However, his narrow perception of privacy did not allow him to realise that in the context of networked surveillance and privacy in public space, privacy and public space have a functional relationship. On the one hand, privacy also serves to protect those aspects of public space connected to political participation and sociability. And, on the other hand, if certain aspects of public space are protected, then opportunities for achieving privacy in public space will also be preserved. In other words, privacy and public space go hand in hand.

In Chapter 6, I examined the level of protection of the right to respect for private life in public stemming from Article 8 ECHR. I have done so in order to answer the seventh and final research sub-question: *Does the right to respect for private life in Article 8 of the European Convention on Human Rights (ECHR) protect privacy in public and, if so, based on what reasoning and to what extent?* I determined that the ECtHR, through a dynamic and broad reading of the right, grants a rather broad level of protection of privacy also in public space. Following the broad manner in which the Court employs three notable categories in its assessment, I examined the matter in a tripartite structure – distinguishing between space, activity and data. As such, I spoke of 'privacy in public' rather than 'privacy in public space' in this Chapter. First, I examined the relevance of space in the Court's assessment whether an interference with Article 8 took place. I established that the place of intrusion does not play a key role in this. Since one of the main purposes of Article 8 is to protect the right to establish and develop relationships with others, the Court has recognised a right to lead a private social life that includes professional activities as well as activities taking place in a public context. Instead, the Court puts more emphasis on the type of activity (private or public) and, particularly, the question whether data relating to private life of an individual have been stored and/or analysed, allowing for possible (further) use. In general, the scope Article 8 does not include 'public activities', that is activities, in which one voluntarily exposes oneself and, which one does not carry out purely or primarily for personal fulfilment (leading to little or no reasonable expectations of privacy). This includes demonstrations and other political activities in public space.

Following this discussion, I examined the circumstances under which intrusion into private life may be considered warranted and legitimate, as follows from Article 8(2) ECHR and in regard to positive obligations of the state. This type of balancing exercise in relation to privacy has been referred to as the 'knock-down argument' (Nissenbaum, 1998), according to which privacy is easily outweighed by broader societal interests, such as security. The ECtHR, however, has made clear that even in cases of minor

interferences with Article 8 (such as with video surveillance of innocuous activities in public space that records data), surveillance must adhere to the general principles against arbitrary interference (e.g. *Uzun v. Germany* [2010]; *Vukota-Bojić v. Switzerland* [2016]). In the concluding part of this Chapter, I briefly examined the *SLL* through the lens of Article 8. While a longer assessment would be needed in order to speculate about the case with more authority, I nevertheless posit that the brief assessment suggests a possibility that the ECtHR might find the Netherlands either in breach of its positive obligations (for not having struck a fair balance between the opposing interests) or that the measures in question are not in accordance with the law or necessary in a democratic society.

In the concluding chapter (Chapter 7), my general aim was to further privacy scholarship that is emphasising privacy's broader societal and political value, and to do this in the particular context of privacy in public space. In this final Chapter, I thus answer the main research question of this dissertation: *How can and should we conceptualise privacy in public space, especially within the context of surveillance in smart cities and living labs?*

In the first part of the chapter, I offered a rough outline of an original conceptualisation of 'privacy *for* public space' (PfP). This is needed, I argued, because contemporary general conceptualisations of privacy, while broad enough to encompass the various risks stemming from surveillance in public space, are also very abstract, offering few concrete suggestions or starting points in order to be applied in law. While the elusiveness of the concept of privacy can generally be seen as positive in theory, this can be a hindrance in relation to law, where a certain level of precision and concreteness is needed. Furthermore, the specific context (or manifestation) of privacy in public space in connection to surveillance within living labs and smart cities, comes with a particular and often overlooked focus – that is, on the social and political aspects of privacy, which are broadly in line with the values of sociability and political participation connected to public space. As mentioned above, privacy and public space have a particular functional relationship and work together. A more concretely situated conceptualisation of privacy in public space, might thus allow for the emergence of new elements or strengthened arguments in the analysis and, thus, a better appraisal of the concept.

Thus, in this chapter I attempted a synthesis by combining perspectives of privacy and public space (and, to a certain extent, surveillance) in order to explore how privacy in public space can and should be conceptualised so as to also address the social and political significance of public places. This has led me to offer a rough conceptualisation

of 'privacy *for* public space', which can serve as groundwork for further normative analyses of how the right to privacy applies or should apply in multiple-use public spaces. The concept of privacy for public space (PfP) is the result of the attribution of certain attributes of public space to the self-development dimension of privacy. This is based on the insight that in order for individuals to develop into autonomous beings (both personally and politically), they need to be able to participate in the informal life of the community as well as in the formal civic life of the public spheres. While public space is certainly not only a space of politics, it is also 'a space constituted *in* and *through* privacy' (Staeheli & Mitchell, 2004, pp. 149–150), one should also point out the other side of the coin: certain aspects of privacy (particularly those relating to the self-development dimension) are in turn constituted *in* and *through* public space.

My conceptualisation thus strengthens the point already made in privacy theory that privacy needs to protect the possibility to develop and maintain social and political relations. But it also goes further by arguing that in order for a person to be able to develop herself in such a way certain attributes of public space itself – relating both to public space as a sociable space and as political space – need to be protected as well. Based on preceding chapters, particularly Chapters 3, 4 and 5, I have identified six attributes that need protection: openness of access, absence of exclusivity of control, multiple use, tolerance of a level of disorder, anonymity and allowing for dissent. This vision of PfP therefore allows us to better acknowledge the interconnectedness of the value of privacy on public space – its Janusian form: with one side it looks toward the individual and with the other it overlooks society and democratic politics. Yet, rather than leading to opposition, these two sides work together and strengthen each other. PfP also furthers the argument concerning the infrastructural role of privacy in enabling a more secure and fuller exercise of other values, rights and freedoms, such as the plurality, tolerance, freedom of assembly and association, and freedom of expression. And it does so by making more concrete *what* precisely is to be protected in order to preserve both the possibility for an individual to develop oneself in public space as well the sociability of and political participation in public space. This is an important task, especially as this aspect of privacy law has not yet been recognised in legal theory or case law.

This analysis has also provided a more solid foundation for the discussion on regulation of surveillance in public space. In the second part of the Chapter, I briefly examined the possibilities for regulation of surveillance of public space within smart cities and living labs by looking at Morgan and Yeung's (2007) five Cs of regulation: Command, Competition, Consensus, Communication, and Code. In this last part of the Chapter, I came back to the first part of this dissertation – the *Stratumseind Living Lab*,

positing that the *SLL* itself is a hybrid regulatory tool, trying to combine competition, communication and consensus types of tools. The *SLL*, as I have shown in the analysis in Chapter 1, however, comes with several shortcomings and is in need of regulation of its own. I realise that the above brief reflections on various regulatory tools may sound somewhat sceptical of the potential for regulators to successfully address the possible negative effects of surveillance in smart cities and living labs. This is so primarily because the regulatory challenges of smart cities are significant, complex, and widespread. As Katell et al. (forthcoming 2019, p. 39) put it: 'they cannot be addressed by some magic bullet to be found in law, social norms or architecture.' In fact, a combination of several tools, the law, consensus, communication and architecture in particular, will be needed, if the possibility of achieving privacy *in* or, rather, *for* public space is to be achieved and preserved in the new environments of living labs and smart cities. In the above brief discussion on the possibilities and limitations of particular tools in the context of regulating surveillance in smart cities and living labs, I find two tools more promising than others: command (law) and code (architecture). In particular, I found most promising administrative law-type of solutions (e.g. reporting and complaint mechanisms, internal auditing, ombudswomen, special councils, chief privacy officers, obligatory disclosure mechanisms, a focus on decisions that affect people's lives, and adequate funds and powers) and architectural design (both relating to software and physical space) in regard to designing-in dynamic possibilities both for achieving privacy (in accordance with Altman's theory of privacy as a dynamic boundary-management process; see Chapter 3) as well as preserving the identified attributes of public space. Of course, each tool is still in need of a fine-grained and contextualised set of policy interventions, particularly in relation to smart city and living lab initiatives, different geographic and social situations and particular sets of power relations. This dissertation has, hopefully, set a solid foundation for such further work.

LITERATURE

Primary sources

Algemene Plaatselijke Verordening (APV) Eindhoven 2018 (General Municipal Ordinance Eindhoven; Netherlands).

Algemene Plaatselijke Verordening (APV) Rotterdam 2012 (General Municipal Ordinance Rotterdam; Netherlands).

The Anti-Social Behaviour, Crime and Policing Act 2014 (c. 12) (England and Wales).

The Convention for the protection of individuals with regard to automatic processing of personal data, ETS No.108, Strasbourg, 28 January 1981 (1981 CoE Convention)

The Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950 (European Convention on Human Rights).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Gemeentewet 1992 [BWBR0005416] 14 February 1992 (Municipalities Act; Netherlands).

Public Order Act 1986 (c. 64) (England and Wales).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in Paris on 10 December 1948 as Resolution 217 A.

Wet openbare manifestaties 1998 [BWBR0004318] 20 April 1988 (Public Events Act; Netherlands).

ECtHR case law

Altay v. Turkey (no. 2) (2019) Application no. 11236/09.

Amann v. Switzerland (2000) Application no. 27798/95.

Antović and Mirković v. Montenegro (2018) Application no. 70838/13.

Appleby and others v. UK (2003), Application no. 44306/98.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2007) Application no. 62540/00.

Axel Springer AG v. Germany (2012) Application no. 39954/08.

Bărbulescu v. Romania (2017) Application no. 61496/08.

Botta v. Italy (1998) Application no. 21439/93.

Boulois v. Luxembourg (2010) Application no. 37575/04.

Bruggeman and Scheiten v. Germany (1976) App. 6959/75, DR vol. 10.

Buck v. Germany (2005) Application no. 41604/98.

Buckley v. UK (1996) Application no. 20348/92.

Catt v. UK (2019) Application no. 43514/15.

Codarcea v. Romania (2009) Application no. 31675/04.

Copland v. the United Kingdom (2007) Application no. 62617/00.

Craxi v. Italy (2000) Application no. 25337/94.

Demades v. Turkey (2003), Application no. 16219/90.

Friedl v. Austria (1994), Application no. 28/1994/475/556.

Friend and the Countryside Alliance and others v. UK (2009) Applications nos. 16072/06 and 27809/08.

Gillan and Quinton v. UK (2010) Application no. 4158/05.

Gorzelik and others v. Poland (2004) Application no. 44158/98.

Halford v. UK (1997) Application no. 20605/92.

Handyside v. UK (1976) Application no. 5493/72.

Hatton and others v. UK (2003) Application no. 36022/97.

Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium (1998) Applications nos. 32200/96 and 32201/96, Decisions and Reports [DR] 92-B.

Kennedy v. UK (2010) Application no. 26839/05.

Khmel v. Russia (2014) Application no. 20383/04.

Khuzhin and Others v. Russia (2009) Application no. 13470/02.

Klass and Others v. Germany (1978) Application no. 5029/71.

Köpke v. Germany (2000) no. 420/07.

K.U. v. Finland (2009) Application no. 2872/02.

Leander v. Sweden (1987) Application no. 9248/81.

Liberty and others v. UK (2008) Application no. 58243/00.

López Ribalda and others v. Spain (2018) Applications nos. 1874/13 and 8567/13.

Lupker and others v. the Netherlands (1992) App. 18395/95.

Malone v. UK (1984) Application no. 8691/79.

M.C. v. Bulgaria (2003) Application no. 39272/98.

National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France (2018) Applications nos. 48151/11 and 77769/13.

Niemietz v. Germany (1992) Application no. 13710/88.

Pálomo Sanchez and others v. Spain (2011) Applications nos. 28955/06, 28957/06, 28959/06 and 28964/06. Art. 10

Peck v. UK (2003) Application no 44647/98.

Peev v. Bulgaria (2007) Application no. 64209/01.

Perry v. UK (2003) Application no. 63737/00, § 33.

P.G. and J.H. v. the UK (2001) Application no. 44787/98.

Pretty v. UK (2002) Application no. 2346/02.

Reklos and Davourlis v. Greece (2009) Application no. 1234/05.

Rotaru v. Romania (2000) Application no. 28341/95.

S.A.S. v. France (2014) Application no. 43835/11.

Sciacca v. Italy (2005) Application no. 50774/99.

Segerstedt-Wiberg and others v. Sweden (2009) Application No. 62332/00.

Shimovolos v. Russia (2011) Application no. 30194/09.

Smirnova v. Russia (2003) Applications nos. 46133/99 and 48183/99.

Söderman v. Sweden (2013) Application no. 5786/08.

Sorvisto v. Finland (2009) Application no. 19348/04.

Uzun v. Germany (2010) Application No. 35623/05.

von Hannover v. Germany (2004) Application no. 59320/00.

von Hannover v. Germany (no. 2) (2012) Applications nos. 40660/08and 60641/08.

Vukota-Bojić v. Switzerland (2016) Application no. 61838/10.

Weber and Saravia v. Germany (2006) Application no. 54934/00.

Wieser and Bicos Beteiligungen GMBH v. Austria (2007) Application no. 74336/01.

X v. Iceland (1976) App. 6825/74, Decisions and reports [DR], vol. 5.

X v. UK (1973) Application no. 5877/72, 16 Y b.

X and Y v. the Netherlands (1985) Application no. 8978/80.

Z v. Finland (1997) Application no. 22009/93.

Zakharov v. Russia (2015) Application no. 47143/06.

Other case law

BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 *('Volkszählungsurteil').*

BVerfGE 6, 32, Urteil vom 16. Januar 1957 - 1 BvR 253/56.

BVerfGE 27, 1, Beschluß vom 16. Juli 1969 - 1 BvL 19/63.

BVerfGE 27, 344, Beschluß vom 15. Januar 1970 - 1 BvR 13/68.

BVerfGE 32, 373, Beschluß vom 8. März 1972 - 2 BvR 28/71.

BVerfGE 43, 238, Beschluß vom 31. Januar 1973 - 2 BvR 454/71.

Carpenter v. United States, 138 S. Ct. 2206 (2018).

CIN Properties Ltd. V Rawlins [1995] 2 EGLR 130.

Entick v. Carrington Camden (1765), 19 State Trials 1045.

Katz v. United States, 389 U.S. 347 (1967).

Prince Albert v. Strange [1849] 1 McN & G 25.

Riley v. California, 134 S. Ct. 2473 (2014).

United States v. Jones, 565 U.S. 400 (2012).

Secondary sources

Agamben, G. (2000). *Means Without End: Notes on Politics*. Minneapolis: University of Minnesota Press.

Agamben, G. (2005). *State of exception*. Chicago: The University of Chicago Press.

Agamben, G. (2011). *Nudities*. Stanford: Stanford University Press.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, *22*(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). Retrieved from https://firstmonday.org/article/view/2142/1949;

Albrechtslund, A., & Dubbeld, L. (2005). The plays and arts of surveillance: studying surveillance as entertainment. *Surveillance and Society*, *3*(2–3), 216–221.

Albrechtslund, A., & Lauritsen, P. (2013). Spaces of everyday surveillance: unfolding an analytical concept of participation. *Geoforum*, *49*, 310–316. https://doi.org/10.1016/j.geoforum.2013.04.016

Alexy, R. (2010). *A theory of constitutional rights*. New York: Oxford University Press.

Allen, A. (1988). *Uneasy access*. New Jersey: Rowman & Littlefield Publishers.

Allen, A. (2011). *Unpopular privacy: what must we hide?* New York: Oxford University Press.

Allen, A., & Rotenberg, M. (Eds.). (2016). *Privacy law and society* (Third). New York: West Academic Publishing.

Altman, I. (1975). *The environment and social behaviour: privacy, personal space, territory and crowding*. Monterey: California: Books/Cole publishing.

Altman, I. (1976). Privacy: "a conceptual analysis." *Environment and Behavior*, *8*(1), 7–29.

Altman, I., & Zube, E. H. (Eds.). (1989). *Public places and spaces* (First). Plenum press.

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television and New Media*, *16*(1), 19–36. https://doi.org/10.1177/1527476414541552

Anthopoulos, L. G. (2015). Understanding the smart city domain: a literature review. In M. Rodríguez-Bolívar (Ed.), *Transforming city governments for successful smart cities* (pp. 9–21). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-03167-5_2

Antonsich, M. (2010). Meanings of place and aspects of the Self: an interdisciplinary and empirical account. *GeoJournal*, *75*(1), 119–132. https://doi.org/10.1007/s10708-009-9290-9

Ardrey, R. (2014). *The Territorial Imperative: A Personal Inquiry into the Animal Origins of Property and Nations*. New York: StoryDesign Limited.

Arendt, H. (1998). *The human condition* (Second). Chicago: The University of Chicago Press.

Arendt, H. (2006). *On revolution*. London: Penguin Books.

Ariès, P. (1989). Introduction. In P. Ariès, G. Duby, & R. Chartier (Eds.), *A history of private life: passions of the Renaissance, vol. 3* (pp. 1–12). Cambridge: Massachusetts: The Belknap Press.

Ariès, P., & Duby, G. (Eds.). (1988). *A history of private life: revelations of the medieval world, vol. 2*. Cambridge: Massachusetts: The Belknap Press.

Ariès, P., Duby, G., & Chartier, R. (Eds.). (1989). *A history of private life: passions of the Renaissance, vol. 3*. Cambridge: Massachusetts: The Belknap Press.

Ariès, P., Duby, G., & Perrot, M. (Eds.). (1990). *A history of private life: from the fires of revolution to the great war, vol. 4*. Cambridge: Massachusetts: The Belknap Press.

Ariès, P., Duby, G., & Prost, A. (Eds.). (1991). *A history of private life: riddles of identity in modern times, vol. 5*. Cambridge: Massachusetts: The Belknap Press.

Arnstein, S. R. (1969). A ladder of citizen participation. *Journal of the American Institute of Planners*, *35*(4), 216–224. https://doi.org/10.1080/01944366908977225

Asenbaum, H. (2018). Anonymity and democracy: absence as presence in the public sphere. *American Political Science Review*, *112*(3), 459–472. https://doi.org/10.1017/S0003055418000163

Ashworth, A., & Zedner, L. (2014). *Preventive Justice*. Oxford: Oxford University Press.

Aston, V. (2017). State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives. *European Journal of Law and Technology*, *8*(1).

Atos. (2015). CityPulse - using big data for real time incident response management. Retrieved March 23, 2019, from https://atos.net/wp-content/uploads/2016/06/atos-ph-eindhoven-city-pulse-case-study.pdf

Augé, M. (2009). *Non-Places: An Introduction to Supermodernity*. London: Verso.

Aurigi, A., & De Cindio, F. (2008). *Augmented Urban Spaces: Articulating the Physical and Electronic City*. Oxon: Routledge.

Austin, L. M. (2019). Re-reading Westin. *Theoretical Inquiries in Law*, *20*(1), 53–82.

Bachelard, G. (2014). *The poetics of space*. London: Penguin Books.

Bachrach, P., & Baratz, M. S. (1962). Two Faces of Power. *The American Political Science Review*, *56*(4), 947–952.

Bailey, K. D. (1994). *Typologies and taxonomies: an introduction to classification techniques*. Thousand Oaks: California: Sage publications.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication and Society*, 12(5), 639–657.

Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body-subject. *Body & Society*, 22(2), 58–81.

Ball, K. (2019). Peers and Prejudice: Neighbourhood Watch in Europe. In K. Ball & W. Webster (Eds.), *Surveillance and democracy in Europe* (pp. 91–107). Oxon: Routledge.

Ball, K., Timan, T., & Webster, W. (2019). Surveillance theory meets participatory theory. In K. Ball (Ed.), *Surveillance and democracy in Europe* (p. 138). Oxon: Routledge.

Ballon, P. (2015). Living Labs. In R. Mansell & P. Hwa Ang (Eds.), *The international encyclopedia of digital communication and society* (pp. 552–556). New York: John Wiley & Sons.

Ballon, P., Pierson, J., & Delaere, S. (2005). Test and experimentation platforms for broadband innovation: examining European practice. In *16th european regional conference by the International Telecommunications Society (ITS 2005)* (p. 22). Porto.

Bannister, J., Fyfe, N. R., & Kearns, A. (1998). Closed circuit television and the city. In C. Norris, J. Moran, & G. Armstron (Eds.), *Surveillance, Closed Circuit Television, and Social Control* (pp. 21–40). Farnham: Ashgate.

Barocas, S., & Nissenbaum, H. (2014). Big Data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the public good: frameworks for engagement* (pp. 44–75). Cambridge: Cambridge University Press.

Barry, A., Born, G., & Weszkalnys, G. (2008). Logics of interdisciplinarity. *Economy and Society*, *37*(1), 20–49. https://doi.org/10.1080/03085140701760841

Bates, J. (2012). "This is what modern deregulation looks like": Co-optation and contestation in the shaping of the UK's Open Government Data Initiative. *The Journal of Community Informatics*, *8*(2). Retrieved from http://www.ci-journal.net/index.php/ciej/article/view/845/916

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

Bauman, Z. (1998). On Glocalization: or Globalization for some, Localization for some Others. *Thesis Eleven*, *54*(1), 37–49. Retrieved from https://journals.sagepub.com/doi/10.1177/072551369805400004

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: a conversation*. Cambridge: Polity press.

Beckett, K., & Herbert, S. (2008). Dealing with disorder: social control in the post-industrial city. *Theoretical Criminology*, *12*(1), 5–30. https://doi.org/10.1177/1362480607085792

Beckett, K., & Herbert, S. (2010a). *Banished: The New Social Control in Urban America*. Oxford: Oxford University Press.

Beckett, K., & Herbert, S. (2010b). Penal boundaries: Banishment and the expansion of punishment. *Law and Social Inquiry*, *35*(1), 1–38. https://doi.org/10.1111/j.1747-4469.2009.01176.x

Belina, B. (2007). From Disciplining To Dislocation. *European Urban and Regional Studies*, *14*(4), 321–336. https://doi.org/10.1177/0969776407081165

Benhabib, S. (Ed.). (1996). *Democracy and difference: contesting the boundaries of the political*. Princeton: New Jersey: Princeton University Press.

Benhabib, S. (2000). The embattled public sphere: Hannah Arendt, Jürgen Habermas, and beyond. In E. Ullmann-Margalit (Ed.), *Reasoning practically* (pp. 164–181). Oxford: Oxford University Press.

Benn, S. I. (1984). Privacy, freedom and respect for persons. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 223–244). Cambridge: Cambridge University Press.

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: policy instruments in global perspective*. Cambridge: Massachusetts: The MIT press.

Bentham, J. (2010). *The panopticon writings*. London: Verso.

Bergvall-Kåreborn, B., Eriksson, C. I., Ståhlbröst, A., & Svensson, J. (2009). A milieu for innovation-defining living labs. In K. R. E. Huizingh, S. Conn, M. Torkkeli, & I. Bitran (Eds.), *2nd ISPIM innovation symposium: simulating recovery - the role of innovation management*. New York. Retrieved from http://www.diva-portal.org/smash/get/diva2:1004774/FULLTEXT01.pdf

Berman, M. (2006). *On the town: one hundred years of spectacle in times square*. Random House.

Beyleveld, D., & Brownsword, R. (2001). *Human dignity in bioethics and biolaw*. Oxford: Open University Press.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorising surveillance: the panopticon and beyond* (pp. 46–68). Devon: Willan Publishing.

Bigo, D. (2008). Security: A Field Left Fallow. In M. Dillon & A. W. Neal (Eds.), *Foucault on Politics, Security and War* (pp. 93–114). Hampshire: Palgrave Macmillan.

Bijker, W. E., & Pinch, T. J. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

Blackburn, R. (2001). The Institutions and Processes of the Convention. In R. Blackburn & J. Polakiewicz (Eds.), *Fundamental Rights in Europe The European Convention on Human Rights and its Member States, 1950-2000* (pp. 3–30). Oxford: Oxford University Press.

Blok, P. (2002). *Het recht op privacy. Een oderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikanse recht*. Den Haag: Boom Uitgevers.

Blomley, N. (2005). Flowers in the bathtub: boundary crossings at the public–private divide. *Geoforum*, *36*, 281–296. https://doi.org/10.1016/j.geoforum.2004.08.005

Boa, K. (2007). Privacy outside the castle: Surveillance technologies and reasonable expectations of privacy in Canadian judicial reasoning. *Surveillance and Society*, *4*(4), 329–345.

Bobbio, N. (1989). *Democracy and dictatorship: the nature and limits of state power*. Cambridge: Polity press.

Boehme-Neßler, V. (2016). Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, *6*(3), 222–229. https://doi.org/10.1093/idpl/ipw007

Bok, S. (1989). *Secrets: on the ethics of concealment and revelation*. New York: Vintage Books.

Borgesius, F. J. Z., Möller, J., Kruikemeier, S., Fathaigh, R., Irion, K., Dobber, T., … de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82–96. https://doi.org/10.18352/ulr.420

Born, G. (2009). The social and the aesthetic: methodological principles in the study of cultural production. In I. Reed & J. C. Alexander (Eds.), *Meaning and method: the cultural approach to sociology* (pp. 77–117). Oxon: Routledge.

Bowker, G. C., & Star, S. L. (2000). *Sorting Things Out Classification and Its Consequences*. Cambridge: Massachusetts: MIT Press.

boyd, danah m. (2011). Dear voyeur, meet Flâneur… Sincerely, social media. *Surveillance and Society*, *8*(4), 505–507.

boyd, danah m., & Ellison, N. B. (2008). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Božovič, M. (2010). Introduction: 'An utterly dark spot''.' In *The panopticon writings* (pp. 1–28). London: Verso.

Bradley, C. M. (1981). Constitutional Protection for Private Papers. *Harvard Civil Rights-Civil Liberties Law Review*, *16*, 461–494.

Brandeis, S. D., & Warren, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Brands, J., & Schwanen, T. (2014). Experiencing and governing safety in the night-time economy: nurturing the state of being carefree. *Emotion, Space and Society*, *11*, 67–78. https://doi.org/10.1016/j.emospa.2013.08.004

Brands, J., Schwanen, T., & van Aalst, I. (2015). Fear of crime and affective ambiguities in the night-time economy. *Urban Studies*, *52*(3), 439–455. https://doi.org/10.1177/0042098013505652

Brenner, N., & Theodore, N. (2002). Cities and the geographies of "actually existing neoliberalism." *Antipode*, *34*(3), 349–379. https://doi.org/10.1111/1467-8330.00246

Brettschneider, C. (2007). *Democratic Rights: The Substance of Self-Government*. Princeton: New Jersey: Princeton University Press.

Brighenti, A. M. (2010a). Democracy and its visibilities. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and democracy* (pp. 51–68). Oxon: Routledge.

Brighenti, A. M. (2010b). *Visibility in social theory and social research*. New York: Palgrave Macmillan.

Brotchie, J., Batty, M., Blakely, E., Hall, P., & Newton, P. (Eds.). (1995). *Cities in competition: productive and sustainable cities for the 21st century*. Melbourne: Longman Australia.

Brown, A. P. (2004). Anti-Social Behaviour, Crime Control and Social Control. *The Howard Journal of Criminal Justice*, *43*(2), 203–211. https://doi.org/10.1111/j.1468-2311.2004.00321.x

Brownsword, R. (2005). Code, control, and choice: why East is East and West is West. *Legal Studies*, *25*(1), 1–21.

Brownsword, R. (2006). Neither East Nor West, Is Mid-West Best? *SCRIPT-Ed*, *3*(1), 15–33. https://doi.org/10.2966/scrip.030106.15

Brunon-Ernst, A. (2012). Deconstructing panopticism into the plural panopticons. In A. Brunon-Ernst (Ed.), *Beyond Foucault: new perspectives on Bentham's panopticon* (pp. 17–42). Surrey: Ashgate.

Brunon-Ernst, A., & Tusseau, G. (2012). Epilogue: the panopticon as a contemporary icon? In A. Brunon-Ernst (Ed.), *Beyond Foucault: new perspectives on Bentham's panopticon* (pp. 185–200). Surrey: Ashgate.

Brunton, F., & Nissenbaum, H. (2013). Political and ethical perspectives on data obfuscation. In M. Hildebrandt & K. De Vries (Eds.), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology* (pp. 171–195). Oxon: Routledge.

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: a user's guide for privacy and protest*. Cambridge: Massachusetts: The MIT press.

Bryman, A. (2012). *Social research methods* (Fourth). Oxford: Oxford University Press.

Burgess, R. G. (1984). *In the field: an introduction to field research*. Oxon: Routledge.

Burkert, H. (2008). Dualities of privacy – An introduction to 'Personal data protection and fundamental rights.' In M. V. Perez Asinari & P. Palazzi (Eds.), *Défis du droit à la protection à la vie privée/Challenges of privacy and data protection law* (pp. 13–23). Bruxelles: Bruylant.

Caragliu, A., Del, C. B. O., & Nijkamp, P. (2009). Smart cities in Europe. In *3rd Central European Conference in Regional Science – CERS, 2009* (pp. 45–59). Amsterdam: VU Amsterdam. Retrieved from https://inta-aivn.org/images/cc/Urbanism/background

Cardullo, P., & Kitchin, R. (2018). Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused'' smart cities in Europe.' *Environment and Planning C: Politics and Space*, *0*(0), 1–18. https://doi.org/10.1177/0263774X18806508

Cardullo, P., Kitchin, R., & Di Feliciantonio, C. (2018). Living labs and vacancy in the neoliberal city. *Cities*, *73*, 44–50. https://doi.org/10.1016/J.CITIES.2017.10.008

Carr, S., Francis, M., Rivlin, L. G., & Stone, A. M. (1995). *Public space*. Cambridge: Cambridge University Press.

Carter, I., Kremer, M. H., & Steiner, H. (2007). *Freedom: A Philosophical Anthology*. Malden: Massachusetts: Blackwell.

Castan, N., Aymard, M., Collomp, A., Fabre, D., & Farge, A. (1989). Community, state, and family: trajectories and tensions. In P. Ariès, G. Duby, & R. Chartier (Eds.), *A history of private life: passions of the Renaissance, vol. 3* (pp. 397–608). Cambridge: Massachusetts: The Belknap Press.

Castan, Y., Lebrun, F., & Chartier, R. (1989). Figures of modernity. In P. Ariès, G. Duby, & R. Chartier (Eds.), *A history of private life: passions of the Renaissance, vol. 3* (pp. 13–160). Cambridge: Massachusetts: The Belknap Press.

Castells, M. (2000). *The rise of the network society, The Information Age: Economy, Society and Culture Vol 1* (Second). Oxford: Blackwell.

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, *3*(2), 405–413. https://doi.org/10.1007/s12394-010-0053-z

Chartier, R. (1989a). Introduction - community, state, and family: trajectories and tensions. In P. Ariès, G. Duby, & R. Chartier (Eds.), *A history of private life: passions of the Renaissance, vol. 3* (pp. 399–402). Cambridge: Massachusetts: The Belknap Press.

Chartier, R. (1989b). Introduction - Figures of modernity. In P. Ariès, G. Duby, & R. Chartier (Eds.), *A history of private life: passions of the Renaissance, vol. 3* (pp. 15–20). Cambridge: Massachusetts: The Belknap Press.

Chatterton, P., & Hollands, R. (2003). *Urban Nightscapes: Youth Cultures, Pleasure Spaces and Corporate Power*. Oxon: Routledge.

Cheney-Lippold, J. (2011). A New Algorithmic Identity. *Theory, Culture & Society*, *28*(6), 164–181. https://doi.org/10.1177/0263276411424420

Chong, D., & Druckman, J. N. (2007). Framing theory. *Annual Review of Political Science*, *10*(1), 103–126. https://doi.org/10.1146/annurev.polisci.10.072805.103054

Christman, J. (2014). *The Inner Citadel: essays on Individual Autonomy* (Second). Brattleboro: Vermont: Echo Point Books & Media.

Clark, H. H. (1983). Making sense of nonce sente. In G. B. D'Arcais Flores & R. Jarvella (Eds.), *The process of understanding language* (pp. 297–331). New York: John Wiley & Sons.

Clarke, A., & Montini, T. (1993). The Many Faces of RU486: Tales of Situated Knowledges and Technological Contestations. *Science, Technology, & Human Values*, *18*(1), 42–78.

Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, *52*, 1373–1437. https://doi.org/10.4324/9781351154161-12

Cohen, J. E. (2007). Cyberspace As / and Space. *Columbia Law Review*, *107*(210), 210–256.

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, *126*(7), 1904–1933. https://doi.org/10.1525/sp.2007.54.1.23.

Cohen, J. E. (2016). The Surveillance–Innovation Complex: The Irony of the Participatory Turn. In D. Barney, G. Coleman, C. Ross, J. Sterne, & T. Tembeck (Eds.), *The Participatory Condition in the Digital Age* (pp. 207–226). Minneapolis: University of Minnesota Press.

Cohen, J. E. (2017). Surveillance vs. privacy: effects and implications. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of surveillance law* (pp. 455–469). Cambridge: Cambridge University Press.

Cohen, J. L. (1997). Rethinking privacy: the abortion controversy. In J. Weintraub & K. Kumar (Eds.), *Public and private in thought and practice: perspectives on a grand dichotomy* (pp. 133–165). Chicago: The University of Chicago Press.

Cohen, J. L. (2004). *Regulating Intimacy: A New Legal Paradigm*. Princeton: New Jersey: Princeton University Press.

Coleman, J. (2005). Pre-modern property and self-ownership before and after Locke: or, when did common decency become a private rather than a public virtue? *European Journal of Political Theory*, *4*(2), 125–145. https://doi.org/10.1177/1474885105050446

Constant, B. (1980). *De la liberté chez les modernes: Écrits politiques*. (M. Gauchet, Ed.). Paris: Le Livre de Poche.

Cornwall, A., & Coelho, V. S. P. (Eds.). (2007). *Spaces for change? The politics of citizen participation in new democratic arenas*. London: Zed Books. Retrieved from http://libproxy.mit.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00916a&AN=mit.001420894&site=eds-live&scope=cite

Crampton, J. W., & Elden, S. (Eds.). (2016). *Space, Knowledge and Power: Foucault and Geography*. Oxon: Routledge.

Crang, M., & Graham, S. (2007). Sentient cities: ambient intelligence and the politics of urban space. *Information Communication and Society*, *10*(6), 789–817. https://doi.org/10.1080/13691180701750991

Crang, M., & Thrift, N. (2000). Introduction. In M. Crang & N. Thrift (Eds.), *Thinking space*. Oxon: Routledge.

Cresswell, T. (2015). *Place: an introduction* (Second). Chichester: West Sussex: Wiley-Blackwell.

Cutler, A. C. (1997). Artifice, ideology and paradox: the public/private distinction in international law. *Review of International Political Economy*, *4*(2), 261–285. https://doi.org/10.1080/096922997347788

D'Arcus, B. (2004). Dissent, public space and the politics of citizenship: riots and the "outside agitator." *Space and Polity*, *8*(3), 355–370.

Dahl, R. A. (1957). The concept of power. *Behavioral Science*, *2*(3), 201–215.

Dalibert, L. (2014). *Posthumanism and somatechnologies: exploring the intimate relations between humans and technologies*. University of Twente. Retrieved from https://ris.utwente.nl/ws/portalfiles/portal/6057325/thesis_L_Dalibert.pdf

Dalla Corte, L., van Loenen, B., & Cuijpers, C. (2017). Personal data protection as a nonfunctional requirement in the smart city's development. In *13th International conference on internet, law & politics, Universitat Oberta de Catalunya, Barcelona, 29-30 June, 2017* (pp. 76–92). Barcelona.

Davies, W. (2015). *The happiness industry: how the government and big business sold us well-being*. London: Verso.

Davis, M. (2006). *City of quartz: Excavating the Future in Los Angeles*. London: Verso.

De Certau, M. (1988). *The practice of everyday life*. Berkeley: University of California Press.

de Freitas, A. C. (2010). Changing spaces: locating public space at the intersection of the physical and digital. *Geography Compass*, *4*(6), 630–643. https://doi.org/10.1111/j.1749-8198.2009.00312.x

de Graaf, F. (1977). *Rechtsbescherming van persoonlijkheid, privéleven, persoonsgegevens*. Tjeenk Willink, Alphen aan den Rijn.

de Graaf, P. (2015, November 23). Een biertje met Big Brother erbij op Stratumseind. *De Volkskrant*. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/een-biertje-met-big-brother-erbij-op-stratumseind~b3cc767c/

De Hert, P., & Gutwirth, S. (2009). Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In Y. Poullet, S. Gutwith, C. De Terwanghe, & P. De Hert (Eds.), *Reinventing Data Protection?* (pp. 3–45). Dordrecht: Springer.

de Kort, Y. A. W. (2014). Spotlight on aggression. *ILI 2014*, (1), 10–11.

de Kort, Y. A. W. (2015). *Light on and in context*. Eindhoven. Retrieved from www.tue.nl/taverne

de Kort, Y. A. W., Ijsselsteijn, W. A., Haans, A., Lakens, D., & Kalinauskaitė, I. (2014). De-escalate: defusing escalating behaviour through the use of interactive light scenarios. In Y. A. W. de Kort, M. P. J. Aarts, A. Haans, I. Heynderickx, L. M. Huiberts, I. Kalinauskaite, & P. Khademagha (Eds.), *Experiencing light 2014: International conference on the effects of light on wellbeing, 10- 11 November 2014* (pp. 94–97). Eindhoven: Technische Universiteit Eindhoven. Retrieved from https://pdfs.semanticscholar.org/71ed/561bf09ee8bfffb02df9bbdf40576ac55167.pdf

de Kort, Y. A. W., Ijsselsteijn, W. A., Haans, A., Lakens, D., Kalinauskaitė, I., & Schietecat, A. C. (2014). De-escalate: defusing escalating behaviour through the use of interactive light scenarios. In *Experiencing light 2014: International conference on the effects of light on wellbeing, 10- 11 November 2014* (pp. 94–97).

de Wijs, L., Witte, P., & Geertman, S. (2016). How smart is smart? Theoretical and empirical considerations on implementing smart city objectives – A case study of Dutch railway station areas. *Innovation: The European Journal of Social Science Research*, *29*(4), 424–441. https://doi.org/10.1080/13511610.2016.1201758

Dean, M. M. (2010). *Governmentality: Power And Rule In Modern Society*. London: SAGE.

DeCew, J. W. (1997). *In pursuit of privacy: law, ethics and the rise of technology*. Ithaca: Cornell University Press.

DeCew, J. W. (2015). The feminist critique of privacy: past arguments and new social understandings. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: interdisciplinary perspectives* (pp. 85–103). Cambridge: Cambridge University Press.

DeCew, J. W. (2018). Privacy. In *Stanford Encyclopedia of Philosophy*. Retrieved from https://plato.stanford.edu/entries/privacy/

DeLanda, M. (2006). *A new philosophy of society: assemblage theory and social complexity* (First). London: Continuum.

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3–7. https://doi.org/10.2307/778828

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Dell'Era, C., & Landoni, P. (2014). Living Lab: a methodology between user-centred design and participatory design. *Creativity and Innovation Management*, *23*(2), 137–154. https://doi.org/10.1111/caim.12061

den Ouden, H., & Valkenburg, A. C. (2013). Smart urban lighting. In A. Nighten (Ed.), *Real projects for real people* (Volume 3). Rotterdam: The Patching Zone.

Dewey, J. (2016). *The Public and Its Problems: An Essay in Political Inquiry*. Athens: Ohio: Swallow Press.

Dholakia, N., & Zwick, D. (2001). Privacy and Consumer Agency in the Information Age: Between Prying Profilers and Preening Webcams. *Journal of Research for the Consumer*, *1*(1), 31–43. Retrieved from http://www.yorku.ca/dzwick/JMM_whose_identity.pdf

Dilts, A., & Harcourt, B. E. (2008). Discipline, Security, and Beyond: A Brief Introduction. *Carceral Notebooks*, *4*(1), 1–6.

DiMaggio, P. (1997). Culture and cognition. *Annual Review of Sociology*, *23*, 263–287.

Dixon, J., Levine, M., & McAuley, R. (2006). Locating impropriety: street drinking, moral order, and the ideological dilemma of public space. *Political Psychology*, *27*(2), 187–206. https://doi.org/10.1111/j.1467-9221.2006.00002.x

Djaouti, D., Alvarez, J., & Jessel, J.-P. (2011). Classifying serious games: the G/p/s model. In P. Felicia (Ed.), *Handbook of research on improving learning and motivation through educational games: multidisciplinary approaches* (pp. 118–136). Hershey: IGI Global. Retrieved from http://www.ludoscience.com/files/ressources/classifying_serious_games.pdf

Donath, J. (2014). *The social machine: designs for living online*. Cambridge: Massachusetts: MIT press.

Dorresteijn, S. (2012). *The design of our own lives: Technical mediation and subjectivation after Michel Foucault*. University of Twente. https://doi.org/https://doi.org/10.3990/1.9789036534420

Douglas, M. (1978). Judgments on James Frazier. *Daedalus*, *107*.

Doyle, A., Lippert, R., & Lyon, D. (Eds.). (2012). *Eyes Everywhere: The Global Growth of Camera Surveillance*. Oxon: Routledge.

Duby, G. (1987). Foreword. In P. Ariès, G. Duby, & P. Veyne (Eds.), *A history of private life: from pagan Rome to Byzantium, vol. 1* (pp. vii–1). Oxford: The Belknap Press.

Duneier, M. (1994). *Slim's Table: Race, Respectability, and Masculinity*. Chicago: The University of Chicago Press.

Durkheim, É. (2001). *The Elementary Forms of Religious Life*. Oxford: Oxford University Press.

Dutilleul, B., Birrer, F. A. J., & Mensink, W. (2010). Unpacking European Living Labs: analysing innovation's social dimensions. *Central European Journal of Public Policy*, *4*(1), 60–85. Retrieved from https://www.ceeol.com/content-files/document-139748.pdf

Dutton, W. H., Blumler, J. G., & Kraemer, K. L. (Eds.). (1987). *Wired cities: shaping the future of communications*. Boston: G. K. Hall & Co.

Dworkin, G. (1978). Privacy and the law. In J. B. Young (Ed.), *Privacy* (pp. 113–136). Chichester: John Wiley & Sons.

Dworkin, G. (2014). The concept of autonomy. In J. Christman (Ed.), *The inner citadel: essays on individual autonomy* (pp. 54–62). Brattleboro: Vermont: Echo Point Books & Media.

Eberle, E. J. (1997). Human Dignity, Privacy, and Personality inGerman and American Constitutional Law. *Utah Law Review*, *4*(963), 963–1056. https://doi.org/10.3868/s050-004-015-0003-8

Edquist, C. (2001). Innovation policy - A systemic approach. In D. Archibugi & B.-A. Lundvall (Eds.), *The Globalizing Learning Economy: Major Socio-Economic Trends and European Innovation Policy* (pp. 219–238). Oxford: Oxford University Press.

Edwards, L. (2016). Privacy, security and data protection in smart cities: a critical EU law perspective. *European Data Protection Law Review*, *2*(1), 28–58.

Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, *16*(1), 18–84. https://doi.org/10.2139/ssrn.2972855

Eijkman, Q. (2010). Has the Genie Been Let out of the Bottle? Ethnic Profiling in the Netherlands. *Public Space: The Journal of Law and Social Justice*, *5*(2), 1–21. https://doi.org/10.5130/psjlsj.v5i0.1876

Eindhoven, G. (2015). *Businessplan Living Lab Stratumseind*. Eindhoven.

Eindhovense innovatie is voorbeeld voor de rest van het land, staatssecretaris brengt bezoek aan Stratumseind. (2018, November). *Studio 040*. Retrieved from https://www.studio040.nl/eindhovense-innovatie-is-voorbeeld-voor-de-rest-van-het-land-staatssecretaris-brengt-bezoek-aan-stratumseind/content/item?1109883=

Elden, S. (2001). Politics, philosophy, geography: Henri Lefèbvre in recent Anglo-American scholarship. *Antipode*, *33*(5), 809–825. https://doi.org/10.1111/1467-8330.00218

Elias, N. (1978). *The civilizing process: the history of manners*. New York: Urizen Books.

Ellin, N. (Ed.). (1997). *The architecture of fear*. New York: Princeton Architectural Press.

Elmer, G. (2003). A Diagram of Panoptic Surveillance. *New Media & Society*, *5*(2), 231–247. Retrieved from http://www.academia.edu/312809/A_Diagram_of_Panoptic_Surveillance

Elshtain, J. B. (1997). The displacement of politics. In J. Weintraub & K. Kumar (Eds.), *Public and private in thought and practice: perspectives on a grand dichotomy* (pp. 166–181). Chicago: The University of Chicago Press.

Entrikin, J. N. (2002). Democratic place-making and multiculturalism. *Geografiska Annaler. Series B, Human Geography*, *84*(1), 19–25.

Eriksson, M., Niitamo, V.-P., & Kulkki, S. (2005). *State-of-the-art in utilizing Living Labs approach to user-centric ICT innovation-a European approach*. Lulea.

Estes, Z., & Glucksberg, S. (2000). Interactive property attribution in concept combination. *Memory and Cognition*, *28*(1), 28–34. https://doi.org/10.3758/BF03211572

Etzioni, A. (1999). *The limits of privacy*. New York: Basic Books.

Evans, J., Karvonen, A., & Raven, R. (Eds.). (2016). *The experimental city*. London: Routledge. https://doi.org/10.4324/9781315719825-1

Featherstone, M., Lash, S., & Robertson, R. (Eds.). (1995). *Global modernities*. London: Sage.

Feinberg, J. (1984). *Harm to others: the moral limits of the criminal law*. Oxford: Oxford University Press.

Feldman, D. (1997). The developing scope of Article 8 of the European Convention on Human Rights. *European Human Rights Law Review*, *3*, 265–274.

Feldman, D. (2002). *Civil Liberties and Human Rights in England and Wales* (Second). Oxford: Oxford University Press.

Fennwick, H. (2017). *Fenwick on Civil Liberties & Human Rights*. Oxon: Routledge.

Ferreira, G. B. (2015). Joining the Spheres: The Smartphone between Public and Private. In J. R. Carvalheiro & A. S. Tellería (Eds.), *Public/private: Mobile and Digital Communication: Approaches to Public and Private* (pp. 159–171). Covilhã: LabCom Books. Retrieved from http://www.labcom-ifp.ubi.pt/ficheiros/20150707-2015_12_public_private.pdf

Finch, K., & Tene, O. (2016). Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. *Fordham Urban Law Journal*, *41*(5), 1581–1615.

Finch, K., & Tene, O. (2018). Smart Cities: Privacy, Transparency, and Community. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 125–148). Cambridge: Cambridge University Press.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology*, *29*(4), 307–312. https://doi.org/10.1007/s13347-016-0220-8

Ford, S. M. (2011). Reconceptualizing the public/ private distinction in the age of information technology. *Information Communication and Society*, *14*(4), 550–567. https://doi.org/10.1080/1369118X.2011.562220

Foucault, M. (1986). Of other spaces: utopias and heterotopias. *Diacritics*, *16*(1), 22–27.

Foucault, M. (1991a). *Discipline and punish: the birth of the prison*. London: Penguin Books.

Foucault, M. (1991b). *The Foucault effect: studies in governmentality*. (G. Burchell, C. Gordon, & P. Miller, Eds.). Chicago: The University of Chicago Press.

Foucault, M. (1998). *The History of Sexuality: the Will to Knowledge, vol. 1*. London: Penguin Books.

Foucault, M. (2002). *Power: the essential works of Foucault 1954–1984, vol. 3*. (J. D. Faubion, Ed.). London: Penguin Books.

Foucault, M. (2006). *Psychiatric power: lectures at the Collège de France 1973-1974*. (J. Lagrange, Ed.). New York: Palgrave Macmillan.

Foucault, M. (2007). *Security, territory, population: lectures at the Collège de France 1977-1978*. New York: Picador.

Fox, J. D., & Stinnett, T. A. (1996). The effects of labeling bias on prognostic outlook for children as a function of diagnostic label and profession. *Psychology in the Schools*, *33*(2), 143–152. https://doi.org/10.1002/(sici)1520-6807(199604)33:2<143::aid-pits7>3.3.co;2-#

Fraser, N. (1990). Rethinking the public sphere: a contribution to the critique of actually existing democracy. *Social Text*, *25/26*, 56–80.

Fried, C. (1984). Privacy (a moral analysis). In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 203–222). Cambridge: Cambridge University Press.

Friedrich, C. J. (1971). Secrecy versus privacy: the democratic dilemma. In J. R. Pennock & J. W. Chapman (Eds.), *Privacy (Nomos XIII)* (pp. 105–120). New York: Atherton Press.

Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review*, *52*(5), 1461. https://doi.org/10.2307/1229519

Froomkin, A. M. (2017). Privacy impact notices to address the privacy pollution of mass surveillance. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in public space: conceptual and regulatory challenges* (pp. 184–210). Cheltenham: Edward Elgar Publishing.

Fyfe, N. R., & Bannister, J. (1998). The "eyes upon the street": closed circuit television surveillance and the city. In N. R. Fyfe (Ed.), *Images of the Street: Planning, Identity, and Control in Public Space* (pp. 254–267). London: Routledge.

Gabrys, J. (2014). Programming environments: environmentality and citizen sensing in the smart city. *Environment and Planning D: Society and Space*, *32*(1), 30–48. https://doi.org/10.1068/d16812

Gal, S. (2002). A Semiotics of the Public/Private Distinction. *Differences: A Journal of Feminist Cultural Studies*, *13*(1), 77–95. https://doi.org/10.1215/10407391-13-1-77

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy and Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gallie, W. B. (1956). Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, *56*, 167–198.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421–471. https://doi.org/10.2307/795891

Gehl, J. (2011). *Life between buildings: using public space*. (I. Press, Ed.). Washington, DC.

Gellert, R. (2020). *The risk based approach to data protection (forthcoming)*. Oxford: Oxford University Press.

Gemeente Eindhoven. (2016). *Uitvoeringsprogramma Eindhoven Smart Society*. Eindhoven. Retrieved from https://eindhoven.raadsinformatie.nl/document/4094498/1/document

Genesereth, M., & Nilsson, N. (1987). *Logical Foundations of Artificial Intelligence*. Palo Alto: CA: Morgan Kaufmann.

Gerety, T. (1977). Redefining privacy. *Harvard Civil Rights-Civil Liberties Law Review*, *12*(2), 233–296.

Gerstein, R. S. (1978). Intimacy and Privacy. *Ethics*, *89*(1), 76–81.

Gibson-Graham, J. K. (2006). *The end of capitalism (as we know it): a feminist critique of political economy*. Minneapolis: University of Minnesota Press.

Gilliom, J. (2006). Struggling with surveillance: resistance, consciousness, and identity. In K. D. Haggerty & E. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 111–140). Toronto: University of Toronto Press.

Gilliom, J., & Monahan, T. (2013). *SuperVision: an introduction to the surveillance society*. Chicago: The University of Chicago Press.

Gillis, A. R. (1979). Coping with crowding: Television, patterns of activity, and adaptation to high density environments. *Sociological Quarterly*, *20*(2), 267–277.

Giroux, H. A. (2005). *Against the new authoritarianism*. Winnipeg: Arbiter Ring Publishing.

Gitelman, L. (Ed.). (2013). *"Raw Data" Is an Oxymoron*. Cambridge: Massachusetts: MIT Press.

Godard, O., Henry, C., Lagadec, P., & Michel-Kerjan, E. (2002). *Traité des nouveaux risques*. Paris: Gallimard.

Goffman, E. (1959). *The presentation of self in everyday life*. New York: Anchor books.

Goffman, E. (1966). *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York: Free Press.

Goffman, E. (1971). *Relations in public: microstudies in the public order*. London: Allen Lane.

Gómez-Arostegui, H. T. (2005). Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations. *California Western International Law Journal*, *35*(2), 153–202.

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht: Springer.

Goold, B. J. (2009). Surveillance and the political value of privacy. *The Amsterdam Law Forum*, *1*(4), 3–6.

Goold, B. J. (2010). How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy. *Surveillance in a Constitutional Government*, *18*(2000), 38–48. Retrieved from http://papers.ssrn.com/abstract=1876069

Gove, W. R., & Hughes, M. (1980). The Effects of Crowding Found in The Toronto Study: Some Methodological and Empirical Questions. *American Sociological Review*, *45*(5), 864–870.

Graham, S. (2007). *Architectures of Fear: Terrorism and the Future of Urbanism in the West*.

Graham, S., & Marvin, S. (1999). Planning cybercities: integrating telecommunications into urban planning. *Town Planning Review*, *70*(1), 89. https://doi.org/10.3828/tpr.70.1.w34454x3475g2858

Graham, S., & Murakami Wood, D. (2003). Digitizing surveillance : categorization , space ,. *Critical Social Policy*, *23*(2), 227–248.

Gray, K., & Gray, S. F. (1994). Civil rights, civil wrongs and quasi-public space. *European Human Rights Law Review*, *4*, 46–102.

Greenfield, A. (2013). *Against the smart city (the city is here for you to use book 1)*. London: Verso.

Gutwirth, S. (2002). *Privacy and the information age*. Lanham: Maryland: Rowman & Littlefield.

Habermas, J. (1992). *Postmetaphysical thinking: philosophical essays*. Cambridge: Massachusetts: The MIT press.

Habermas, J. (2015). *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge: Polity press.

Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. In D. Lyon (Ed.), *Theorising surveillance: the panopticon and beyond* (pp. 23–45). Devon: Willan Publishing.

Haggerty, K. D. (2014). Surveillance, crime and the police. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 235–243). Oxon: Routledge.

Haggerty, K. D., & Ericson, E. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Hall, E. T. (1990). *The hidden dimension*. New York: Anchor books.

Hall, P. (1995). Towards a general urban theory. In J. Brotchie, M. Batty, E. Blakely, P. Hall, & P. Newton (Eds.), *Cities in competition: productive and sustainable cities for the 21st century* (pp. 3–32). Melbourne: Longman Australia.

Halpern, O., LeCavalier, J., Calvillo, N., & Pietsch, W. (2013). Test-bed urbanism. *Public Culture*, *25*(2 70), 272–306. https://doi.org/10.1215/08992363-2020602

Hansen, K. V. (1997). Rediscovering the social: visiting practices in antebellum New England and the limits of the public/private dichotomy. In J. Weintraub & K. Kumar (Eds.), *Public and private in thought and practice: perspectives on a grand dichotomy* (pp. 268–302). Chicago: The University of Chicago Press.

Haque, U. (2012). What is a city that it would be "smart"? *City in a Box*, *34*, 140–141. Retrieved from http://www.haque.org.uk/papers/V34_page_140-142_Usman_Haque.pdf

Harcourt, B. E. (2014). *Digital Security in the Expository Society: Spectacle, Surveillance, and Exhibition in the Neoliberal Age of Big Data* (Columbia Public Law Research Paper No. 14-404). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2455223

Harris, D., O'Boyle, M., & Bates, E. (2018). *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights*. Oxford: Oxford University Press.

Hartzog, W., Conti, G., Nelson, J., & Shay, L. A. (2015). Inefficiently Automated Law Enforcement. *Michigan State Law Review*, *1763*, 1763–1796. Retrieved from https://digitalcommons.law.msu.edu/lr/vol2015/iss5/2

Harvey, D. (1996). *Justice, nature and the geography of difference*. Malden: Massachusetts: Blackwell.

Harvey, D. (2008). The Right to the City. *New Left Review*, *53*(Sept/Oct), 23–40. https://doi.org/10.1080/13604819608713449

Heidegger, M. (1971). Building dwelling thinking. In *Poetry, language, thought* (pp. 145–161). New York: Harper and Row.

Hentschel, C. (2015). *Security in the bubble: navigating crime in urban South Africa*. Minneapolis: University of Minnesota Press.

Hier, S. P. (2003). Probing the surveillant assemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance and Society*, *3*(1), 399–411.

Hildebrand, D. (2008). *Dewey: A Beginner's Guide*. Oxford: Oneworld.

Hildebrandt, M. (2006a). From data to knowledge: The challenges of a crucial technology. *Datenschutz Und Datensicherheit*, *30*, 548–552.

Hildebrandt, M. (2006b). Privacy and identity. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 43–60). Antwerp: Intersentia. Retrieved from https://ria.ua.pt/handle/10773/1930

Hildebrandt, M. (2008a). A vision of Ambient Law. In R. Brownsword & K. Yeung (Eds.), *Regulating Technologies* (pp. 175–191). Portland: Oregon: Bloomsbury.

Hildebrandt, M. (2008b). Defining Profiling: A New Type of Knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen: cross-disciplinary perspectives* (pp. 17–29). Dordrecht: Springer.

Hildebrandt, M. (2011). Legal Protection by Design: Objections and Refutations. *Legisprudence*, *5*(2), 223–248.

Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, *73*(3), 428–460. https://doi.org/10.1111/j.1468-2230.2010.00806.x

Hill, D. (2013). On the smart city; or, a "manifesto" for smart citizens instead. Retrieved March 24, 2019, from https://www.cityofsound.com/blog/2013/02/on-the-smart-city-a-call-for-smart-citizens-instead.html

Himma, K. E. (2007). Privacy Versus Security: Why Privacy is Not an Absolute Value or Right. *San Diego Law Review*, *44*(4), 859–922.

Hirsch, D. (2005). Is Privacy Regulation the Environmental Law of the Information Age? In K. Strandburg & D. S. Raicu (Eds.), *Privacy and technologies of identity: a cross-disciplinary conversation* (pp. 239–253). New York: Springer.

Hoekstra, D. (2017, December). Netwerk van hypermoderne camera's op Stratumseind in Eindhoven gaat politie helpen. Retrieved from https://www.ed.nl/eindhoven/netwerk-van-hypermoderne-camera-s-op-stratumseind-in-eindhoven-gaat-politie-helpen%7B~%7Da1e8acee/

Hoepman, J.-H. (2018). Privacy Design Strategies (The Little Blue Book). *Transactions of the Canadian Society for Mechanical Engineering*, 30. Retrieved from https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

Hollands, R. G. (2008). Will the real smart city please stand up? *City*, *12*(3), 303–320. https://doi.org/10.1080/13604810802479126

Honneth, A. (1995). *The struggle for recognition: the moral grammar of social conflicts*. Cambridge: Polity press.

Hubbard, P., & Kitchin, R. (Eds.). (2011). *Key thinkers on space and place*. London: Sage publications.

Hubmann, H. (1967). *Das Persönlichkeitsrecht*. Köln: Böhlau.

Hughes, K. (2012). A Behavioural Understanding of Privacy and its Implications for Privacy Law. *Modern Law Review*, *75*(5), 806–836. https://doi.org/10.1111/j.1468-2230.2012.00925.x

Hunt, C. D. L. (2011). Conceptualizing Privacy and Elucidating its importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort. *Queen's Law Journal*, *37*(1), 167–219. Retrieved from http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/queen37&section=8%0Ahttp://0-search.ebscohost.com.aupac.lib.athabascau.ca/login.aspx?direct=true&db=edshol&AN=hein.journals.queen37.8&site=eds-live

Hunt, L., & Hall, C. (1990). The curtain rises. In P. Ariès, G. Duby, & M. Perrot (Eds.), *A history of private life: from the fires of revolution to the Great War* (pp. 7–94). Cambridge: Massachusetts: The Belknap Press.

Hutchinson, T. (2017). Doctrinal research: researching the jury. In D. Watson & M. Burton (Eds.), *Research Methods in Law*. Oxon: Routledge.

Ibbetson, D. (2001). *A historical introduction to the law of obligations*. Oxford: Oxford University Press.

Igo, S. E. (2018). *The known citizen: a history of privacy in modern America*. Cambridge: Massachusetts: Harvard University Press.

Ilouz, E. (2007). *Cold intimacies: the making of emotional capitalism*. Oxford: Polity press.

Inness, J. (1992). *Privacy, intimacy, and isolation*. New York: Oxford University Press.

Ishida, T., & Isbister, K. (Eds.). (2000). *Digital cities: technologies, experiences, and future perspectives*. Berlin: Springer. Retrieved from https://books.google.nl/books?id=c8N89LbQsTQC&dq=Ishida,+T.,+%26+Isbister,+K.+(2000).+Digital+cities:+Technologies,+experiences,+and+future+perspectives.++LNCS:++Springer&lr=&hl=it&source=gbs_navlinks_s

Iveson, K. (2007). *Publics and the city*. Malden: Massachusetts: Blackwell.

Jackson, E. (2001). *Regulating Reproduction: Law, Technology and Autonomy*. Portland: Oregon: Hart Publishing.

Jackson, E. (2016). *Medical Law: Texts and Materials* (Fourth). Oxford: Oxford University Press.

Jackson, P. (1989). *Maps of meaning*. London: Routledge.

Jackson, R. (2005). *Writing the war on terrorism: language, politics, and counter-terrorism*. Manchester: Manchester University Press.

Jacobs, J. (2011). *The death and life of great American cities*. New York: Modern Library.

Jacobson, K. (2010). The experience of home and the space of citizenship. *Southern Journal of Philosophy*, *48*(3), 219–245. https://doi.org/10.1111/j.2041-6962.2010.00029.x

Jenkins, R. (2014). *Social identity*. Oxon: Routledge.

Jiménez, A. C. (2014). The right to infrastructure: a prototype for open source urbanism. *Environment and Planning D: Society and Space: Society and Space*, *32*(2), 342–362. https://doi.org/10.1068/d13077p

Johnson, J. A. (2014). From open data to information justice. *Ethics and Information Technology*, *16*(4), 263–274.

Johnson, R., & Cureton, A. (2016). Kant's Moral Philosophy. In *Stanford Encyclopedia of Philosophy* (Spring 201).

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology*, *36*(2), 220–236.

Johnstone, C. (2017). Penalising Presence in Public Space: Control through Exclusion of the 'Difficult' and 'Undesirable. *International Journal for Crime, Justice and Social Democracy*, *6*(2), 1–16. https://doi.org/10.5204/ijcjsd.v6i2.299

Jonsson Cornell, A. (2016). The right to privacy. In *Max Planck Encyclopedia of Comparative Constitutional Law*. Max Planck Foundation for International Peace and the Rule of Law. Retrieved from http://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156

Kahl, S., & Yates, J. (2009). *Concept Creation, Coherence, and Cohesion*. Retrieved from https://pdfs.semanticscholar.org/e035/ea54558a27f11b0dac0cbd2fcdaffbdeaaa8.pdf

Kaino, M. (2009). Bentham's Concept of Security in a Global Context: The Pannomion and the Public Opinion Tribunal as a Universal Plan. *Journal of Bentham Studies*, *11*(1), 1–29. Retrieved from https://www.ingentaconnect.com/content/uclpress/jbs/2009/00000011/00000001/art00001;jsessionid=usrb64ifv7nt.x-ic-live-01

Kalinauskaitė, I. (2014). *Measuring Stratumseind experience: de-escalate Stratumseind*. Eindhoven: PDEng rapport. Retrieved from https://research.tue.nl/nl/publications/measuring-stratumseind-experience-de-escalate-stratumseind

Kalinauskaitė, I., Haans, A., de Kort, Y. A. W., & Ijsselsteijn, W. A. (2018). Atmosphere in an urban nightlife setting: A case study of the relationship between the socio-physical context and aggressive behavior. *Scandinavian Journal of Psychology*, *59*(2), 223–235. https://doi.org/10.1111/sjop.12431

Kaminski, M. E. (2015). Regulating real-world surveillance. *Washington Law Review*, *90*(3), 1113–1165. Retrieved from https://digital.lib.washington.edu/dspace-law/handle/1773.1/1483

Kaminski, M. E., & Witnov, S. (2015). The conforming effect: first amendment implications of surveillance beyond chilling speech. *University of Richmond Law Review*, *49*, 465–518.

Kant, I. (2012). *Groundwork of the metaphysics of morals*. (M. Gregor & J. Timmermann, Eds.) (Revised). Cambridge: Cambridge University Press.

Kanters, T. (2013). *Living Lab Stratumseind*. Eindhoven. Retrieved from https://veiligheidsalliantie.nl/action/?action=download&id=301

Kanters, T. (2014). *Eindhoven smart light*. Eindhoven. Retrieved from https://www.geonovum.nl/uploads/documents/20140714

Kanters, T. (2016). *Living Lab Stratumseind*. Retrieved from http://www.midpointcsi.nl/powered-by-social-innovation/wp-content/uploads/2016/07/LLTrillion2015.pdf

Kanters, T., & van Hoof, J. (2014). *Stratumseind Living Lab research and design document*.

Kasper, D. V. S. (2007). Privacy as a social good. *Social Thought & Research*, *28*(November), 165–189.

Katell, M., Dechesne, F., Koops, B.-J., & Meessen, P. (2019). Seeing the Whole Picture: Visualising Socio-Spatial Power through Augmented Reality. *Law, Innovation and Technology*, *11*(2).

Keymolen, E. (2016). *Trust on the line*. Erasmus University Rotterdam. Retrieved from hdl.handle.net/1765/93210

King, G., Keohane, R. O., & Verba, S. (1994). *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: New Jersey: Princeton University Press.

Kist, R., & van Noort, W. (2015, August 22). Het misdrijf is al ontdekt voor het gepleegd is. *NRC*. Retrieved from https://www.nrc.nl/nieuws/2015/08/22/het-misdrijf-is-al-ontdekt-voor-het-gepleegd-is-1525496-a270899

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8

Kitchin, R. (2015a). Making sense of smart cities: addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society*, *8*(1), 131–136. https://doi.org/10.1093/cjres/rsu027

Kitchin, R. (2015b). The promise and perils of smart cities. *Society for Computers Law*. Retrieved from https://www.scl.org/articles/3385-the-promise-and-perils-of-smart-cities

Kitchin, R. (2016). The ethics of smart cities and urban science. *Philosophical Transactions A*, *374*. https://doi.org/http://dx.doi.org/10.1098/rsta.2016.0115

Kitchin, R., Cardullo, P., & Feliciantonio, C. Di. (2019). Citizenship, social justice, and the Right to the Smart City. In P. Cardullo, C. Di Feliciantonio, & R. Kitchin (Eds.), *The right to the smart city* (Forthcomin, pp. 1–28). West Yorkshire: Emerald Publishing. Retrieved from https://www.slideshare.net/robkitchin/citizenship-social-justice-and-the-right-to-the-smart-city

Kitchin, R., & Dodge, M. (2011). *Code/space: software and everyday life*. Cambridge: Massachusetts: The MIT press.

Klatt, M. (2011). Positive Obligations under the European Convention on Human Rights. *Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht*, *71*, 691–718.

Klauser, F., Paasche, T., & Söderström, O. (2014). Michel foucault and the smart city: power dynamics inherent in contemporary governing through code. *Environment and Planning D: Society and Space*, *32*(5), 869–885. https://doi.org/10.1068/d13041p

Klijn, E.-H., & Teisman, G. R. (2003). Institutional and strategic barriers to public—private partnership: an analysis of Dutch cases. *Public Money and Management*, *23*(3), 137–146. https://doi.org/10.1111/1467-9302.00361

Kluitenberg, E. (2006). The network of waves: living and acting in a hybrid space. *Open 11: Hybrid Space*, *11*, 6–16. Retrieved from https://www.onlineopen.org/download.php?id=271

Koch, R., & Latham, A. (2012). Rethinking urban public space: accounts from a junction in West London. *Transactions of the Institute of British Geographers*, *37*(4), 515–529.

Kohn, M. (2004). *Brave New Neighborhoods: The Privatization of Public Space*. Oxon: Routledge.

Komninos, N. (2002). *Intelligent cities*. Oxon: Routledge. https://doi.org/10.4324/9780203857748

Koops, B.-J. (2009). Technology and the Crime Society: Rethinking Legal Protection. *Law, Innovation and Technology*, *1*(1), 93–124.

Koops, B.-J. (2010). Law, Technology, and Shifting Power Relations. *Berkeley Technology Law Journal*, *25*(2), 973–1036.

Koops, B.-J. (2014). The Trouble with European Data Protection Law. *International Data Privacy Law*, *4*(4), 250–261.

Koops, B.-J. (2016). *Criminal Investigation and Privacy in Dutch Law* (TILT Law & Technology Working Paper Series). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2888422

Koops, B.-J. (2018). Privacy Spaces. *West Virginia Law Review*, *121*(2), 611–665.

Koops, B.-J., & Galič, M. (2017). Conceptualising space and place: lessons from geography for the debate on privacy in public. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in public space: conceptual and regulatory challenges* (pp. 19–46). Cheltenham: Edward Elgar Publishing.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, *18*(2), 159–171.

Koops, B.-J., Newell, B. C., Roberts, A., Škorvánek, I., & Galič, M. (2018). The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism in Criminal Law. *Law and Social Inquiry*, *43*(4), 1210–1235. https://doi.org/10.1111/lsi.12348

Koops, B.-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, *38*(483), 483–575.

Korsgaard, C. M. (2009). *Self-Constitution: Agency, Identity, and Integrity*. New York: Oxford University Press.

Koskela, H. (2002). Video Surveillance, Gender, and the Safety of Public Urban Space: "Peeping Tom" Goes High Tech? *Urban Geography*, *23*(3), 257–278.

Koskela, H. (2004). Webcams, TV Shows and Mobile phones: Empowering Exhibitionism. *Surveillance & Society*, *2*(2/3), 199–215. Retrieved from http://www.surveillance-and-society.org/cctv.htm

Koskela, H. (2011). "Don't mess with Texas!" Texas virtual border watch program and the (botched) politics of responsibilization. *Crime Media Culture*, *7*(1), 49–65. https://doi.org/10.1177/1741659010369957

Kosta, E. (2017). *Surveilling Masses and Unveiling Human Rights - Uneasy Choices for the Strasbourg Court* (Tilburg Law School Research Paper No. No. 2018-10).

Kourtit, K., Nijkamp, P., & Arribas, D. (2012). Smart cities in perspective – A comparative European study by means of self-organizing maps. *Innovation: The European Journal of Social Science Research*, *25*(2), 229–246. https://doi.org/10.1080/13511610.2012.660330

Kranzberg, M. (1986). Technology and History: "Kranzberg's Laws." *The Johns Hopkins University Press and the Society for the History OfTechnology*, *27*(3), 544–560.

Kudina, O., & Baş, M. (2018). "The end of privacy as we know it": reconsidering public space in the age of Google Glass. In B. C. Newell, T. Timan, & B.-J. Koops (Eds.), *Surveillance, privacy and public space* (pp. 119–140). Oxon: Routledge.

Kumar, K., & Makarova, E. (2008). The Portable Home: The Domestication of Public Space. *Sociological Theory*, *26*(4), 326–343. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1467-9558.2008.00332.x

Kviselius, N. Z., & Andersson, P. (2009). Living Labs as tools for open Innovation. *Communications & Strategies*, *1*(74), 75–94. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1559088

Laclau, E., & Mouffe, C. (2014). *Hegemony and socialist strategy: towards a radical democratic politics* (Second). London: Verso.

Larsen, M., & Piché, J. (2009). Public vigilance campaigns and participatory surveillance after 11 September 2001. In S. P. Hier & J. Greenberg (Eds.), *Surveillance: power, problems, and politics* (pp. 187–202). Vancouver: UBC Press.

Latour, B. (1999). On recalling ANT. *The Sociological Review*, *47*(S1), 15–25. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-954X.1999.tb03480.x

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Law, J. (1994). *Organising modernity: social ordering and social theory*. Oxford: Blackwell.

Lawrence, R. J., & Despres, C. (2004). Introduction: futures of transdisciplinarity. *Futures*, *36*, 397–405. https://doi.org/10.1016/j.futures.2003.10.005

Lees, L. (1998). Urban Renaissance and the Street: Spaces of Control and Contestation. In N. R. Fyfe (Ed.), *Images of the street: planning, identity, and control in public space* (pp. 236–253). Oxon: Routledge.

Lefèbvre, H. (1991). *The production of space*. Wiley-Blackwell.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, *113*(501), 501–546.

Letsas. (2013). The ECHR as a living instrument: its meaning and legitimacy. In A. Føllesdal, B. Peters, & G. Ulfstein (Eds.), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context* (pp. 106–141). Oxford: Oxford University Press.

Lever, A. (2015). Privacy, democracy and freedom of expression. In *Social dimensions of privacy: interdisciplinary perspectives* (pp. 162–180). Cambridge: Cambridge University Press.

Locke, J. (1996). *Essay concerning human understanding*. (K. P. Winkler, Ed.). Indianapolis: Hackett Publishing Company.

Lofland, L. H. (1998). *The public realm: exploring the city's quintessential social territory*. New York: Aldine de Gruyter.

Lombardi, P., Giordano, S., Farouh, H., & Yousef, W. (2012). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, *25*(2), 137–149. https://doi.org/10.1080/13511610.2012.660325

Loucaides, L. G. (1990). Personality and Privacy under the European Convention on Human Rights. *British Yearbook of International Law*, *61*(1), 175–197. https://doi.org/10.1093/bybil/61.1.175

Loukaitou-Sideris, A. (1993). Privatisation of Public Open Space: The Los Angeles Experience. *The Town Planning Review*, *64*(2), 139–167.

Lukes, S. (2005). *Power: A radical view* (Second). London: Red Globe Press.

Lyon, D. (2001). *Surveillance society: monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.), *Theorising surveillance: the panopticon and beyond* (pp. 3–20). Portland: Willan Publishing.

Lyon, D. (2007). *Surveillance studies: an overview*. Cambridge: Polity press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Oxford: Polity press.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 1–12). Oxon: Routledge.

Maas, T., van den Broek, J., & Deuten, J. (2017). *Living labs in Nederland: van open testfaciliteit tot levend lab*. Den Haag.

MacKenzie, D. A. (2006). *An engine, not a camera: how financial models shape markets*. Cambridge: MIT Press. Retrieved from https://books.google.nl/books?id=M3x5tvAwzrQC&dq=Donald+MacKenzie,+An+engine,+not+a+camera:+How+Financial+Models+Shape+Markets&lr=&hl=it&source=gbs_navlinks_s

MacKinnon, C. A. (1987). *Feminism Unmodified: Discourses on Life and Law*. Cambridge: Massachusetts: Harvard University Press.

MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Cambridge: Massachusetts: Harvard University Press.

Macnish, K. (2018). *The ethics of surveillance: an introduction*. Oxon: Routledge.

Madanipour, A. (2003). *Public and private spaces of the city*. Oxon: Routledge.

Madden, D. J. (2010). Revisiting the end of public space: assembling the public in an urban park. *City and Community*, *9*(2), 187–207. https://doi.org/10.1111/j.1540-6040.2010.01321.x

Mahoney, P. (1990). Judicial activism and judicial selfrestraint in the European Court of human rights. *Human Rights Law Journal*, *11*(1/2), 57–88.

Mann, S. (2004). "Sousveillance": inverse surveillance in multimedia imaging. In *MULTIMEDIA '04 Proceedings of the 12th annual ACM international conference on Multimedia* (pp. 620–627).

Mantelero, A. (2017). From group privacy to collective privacy: towards a new dimension of privacy and data protection in the Big Data era. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy* (pp. 139–158). Cham: Springer International Publishing.

Marana, P., Labaka, L., & Sarriegi, J. M. (2018). A framework for public-private-people partnerships in the city resilience-building process. *Safety Science*, *110*(Part C), 39–50. https://doi.org/10.1016/j.ssci.2017.12.011

Marcuse, P. (2006). Security or safety in cities? The threat of terrorism after 9/11. *International Journal of Urban and Regional Research*, *30*(4), 919–929. https://doi.org/10.1111/j.1468-2427.2006.00700.x

Margolis, E., & Laurence, S. (2011). Concepts. In *Stanford Encyclopedia of Philosophy*. Retrieved from https://plato.stanford.edu/entries/concepts/

Markopoulos, P., & Rauterberg, G. W. M. (2000). *Living Lab: a white paper*. *IPO annual progress report* (Vol. 35). Retrieved from http://www.livtom.com/

Marshall, J. (2008). *Personal Freedom Through Human Rights Law? Autonomy, Identity and Integrity Under the European Convention on Human Rights*. Leiden: Martinus Nijhoff Publishers.

Marshall, N. J. (1972). Privacy and environment. *Human Ecology*, *1*(2), 93–110.

Marwick, A. E. (2012). The public domain: social surveillance in everyday life. *Surveillance and Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance and Society*, *1*(1), 9–29.

Massey, D. (1992). Politics and space/time. *New Left Review*, *196*(I), 65–84.

Massey, D. (1994). *Space, place, and gender*. Minneapolis: University of Minnesota Press.

Mattern, S. (2013). Methodolatry and the Art of Measure: the new wave of urban data science. *Places Journal*, (November).

May, J., & Thrift, N. (2001). Introduction. In J. May & N. Thrift (Eds.), *TimeSpace: geographies of temporality* (pp. 1–45). Oxon: Routledge.

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton: New Jersey: Princeton University Press.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: a revolution that will transform how we live, work, and think*. New York: Houghton Mifflin Harcourt. https://doi.org/10.2501/IJA-33-1-181-183

Mc Mahon, C., & Aiken, M. (2014). Privacy as Identity Territoriality: Re-Conceptualising Behaviour in Cyberspace. *Ssrn*, 1–49. https://doi.org/10.2139/ssrn.2390934

McCullough, M. (2006). On the Urbanism of Locative Media. *Places*, *18*(2), 26–29. https://doi.org/10.1029/2005JB003736.

McLuhan, M. (1994). *Understanding media*. Cambridge: Massachusetts: The MIT press.

Mead, G. H. (2015). *Mind, Self, and Society (the definitive edition)*. (C. W. Morris, Ed.). Chicago: The University of Chicago Press.

Mercer, D. (2010, March 10). CDC uses shopper-card data to trace salmonella. *The Denver Post*. Retrieved from https://www.denverpost.com/2010/03/10/cdc-uses-shopper-card-data-to-trace-salmonella/

Merton, R. K. (1968). *Social theory and social structure*. New York: The Free Press.

Meyerowitz, J. (1987). *No Sense of Place: The Impact of Electronic Mediaon Social Behavior*. Oxford: Oxford University Press.

Mihailidis, P., & Viotty, S. (2017). Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in "Post-Fact" Society. *American Behavioral Scientist*, *61*(4), 441–454. https://doi.org/10.1177/0002764217701217

Mill, J. S. (2016). *On liberty and other writings*. (S. Collini, Ed.) (Eleventh). Cambridge: Cambridge University Press.

Miller, A. R. (1971). *The assault on privacy. Computers, data banks, and dossiers*. Ann Arbor: Michigan: University of Michigan Press.

Milligan, M. J. (1998). Interactional Past And Potential: The Social Construction Of Place Attachment. *Symbolic Interaction*, *21*(1), 1–33. https://doi.org/10.1525/si.1998.21.1.1

Mitchell, D. (1995). The End of Public Space? People's Park, Definitions of the Public, and Democracy. *Annals of the Association of American Geographers*, *1*(85), 108–133.

Mitchell, D. (2003). *The Right to the City: Social Justice and the Fight for Public Space*. New York: Guilford Press.

Mitchell, W. J. (1995). *City of bits: space, place, and the infobahn*. Cambridge: Massachusetts: MIT Press.

Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy and Technology*, *30*(4), 475–494. https://doi.org/10.1007/s13347-017-0253-7

Moeckli, D. (2016). *Exclusion from Public Space: A Comparative Constitutional Analysis*. Cambridge: Cambridge University Press.

Mokrosinska, D. (2018). Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy. *Law and Philosophy*, *37*(2), 117–143. https://doi.org/10.1007/s10982-017-9307-3

Mol, C., Khan, O., Aalders, R., & Schouten, N. (2015). *How can Eindhoven become a smart city faster?* Eindhoven. Retrieved from https://aireas.files.wordpress.com/2015/12/spotlight-on-smart-city-eindhoven-final.pdf

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: the case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1–2), 57–70. https://doi.org/10.1080/13511610.2013.723396

Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics*, *16*(4), 515–534. https://doi.org/10.1080/10350330601019769

Monahan, T. (2018). The Image of the Smart City: Surveillance Protocols and Social Inequality. In Y. Watanabe (Ed.), *Handbook of Cultural Security* (pp. 210–226). Cheltenham: Edward Elgar Publishing.

More, B. J. (1984). *Privacy: Studies in Social and Cultural History*. Oxon: Routledge.

Moreham, N. A. (2006). Privacy in public places. *Cambridge Law Journal, 65*(3), 606–635.

Morgan, B., & Yeung, K. (2007). *An introduction to law and regulation: text and materials*. Cambridge: Cambridge University Press.

Morozov, E. (2013). *To save everything, click here: the folly of technological solutionism*. (PublicAffairs, Ed.). New York. Retrieved from https://books.google.nl/books/about/To_Save_Everything_Click_Here.html?id=fdggBahA1qsC&redir_esc=y

Morozov, E., & Bria, F. (2018). *Rethinking the smart city*. New York. Retrieved from www.rosalux-nyc.org

Morsink, J. (2000). *The Universal Declaration of Human Rights: Drafting, Origins & Intent*. Philadelphia: University of Pennsylvania Press.

Mouffe, C. (2013). *Agonistics: thinking the world politically*. London: Verso.

Mouffe, C. (2014). For an agonistic public sphere. In L. Tonder & L. Thomassen (Eds.), *Radical Democracy: Politics Between Abundance and Lack* (pp. 132–132). Manchester: Manchester University Press.

Mowbray, A. (2004). *The Development of Positive Obligations Under the European Convention on Human Rights by the European Court of Human Rights*. Oxford: Hart Publishing.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*, 1–21. https://doi.org/10.1098/rsta.2016.0118

Murakami Wood, D. (2013). What is global surveillance? Towards a relational political economy of the global surveillant assemblage. *Geoforum*, *49*, 317–326. https://doi.org/10.1016/j.geoforum.2013.07.001

Murakami Wood, D. (2015, July). Smart city, surveillance city. *SCL - the Society for Computers and Law*. Retrieved from https://www.scl.org/articles/3405-smart-city-surveillance-city

Murakami Wood, D., Ball, K., Lyon, D., Raab, C., Norris, C., & Wood, D. M. (2006). *A report on the surveillance society*. Retrieved from http://www.rcss.ed.ac.uk/teaching/SSICT/documents/Surveillance_society_summary_final.doc

Murphy, G. L. (1988). Comprehending Complex Concepts. *Cognitive Science*, *12*(4), 529–562. https://doi.org/10.1207/s15516709cog1204_2

Murphy, R. F. (1984). Social distance and the veil. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 34–55). Cambridge: Cambridge University Press.

Naafs, S. (2018, March 1). "Living laboratories": the Dutch cities amassing data on oblivious residents. *The Guardian*.

Nafisi, A. (2015). *Reading Lolita in Tehran*. London: Penguin Books.

Nagel, T. (1998). Concealment and Exposure. *Philosophy & Public AffairsPublic Affairs*, *27*(1), 3–30. https://doi.org/10.1111/j.1088-4963.1998.tb00057.x

Nagel, T. (2002). *Concealment and exposure: and other essays*. Oxford: Oxford University Press.

Nagenborg, M. (2017). Hidden in plain sight. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in public space: conceptual and regulatory challenges* (pp. 47–63). Cheltenham: Edward Elgar Publishing.

Nash, J. C. (2005). From Lavender to Purple: Privacy, Black Women, and Feminist Legal Theory. *Cardozo Women's Law Journal*, *11*(303), 303–330. https://doi.org/10.3868/s050-004-015-0003-8

Neal, Z. (2010). Seeking common ground: three perspectives on public space. In *Proceedings of the Institution of Civil Engineers - Urban Design and Planning* (pp. 59–66). ICE publishing.

Neethling, J. (2005). Personality rights: a comparative overview. *The Comparative and International Law Journal of Southern Africa*, *38*(2), 210–245.

Németh, J., & Hollander, J. (2010). Security zones and New York city's shrinking public space. *International Journal of Urban and Regional Research*, *34*(1), 20–34. https://doi.org/10.1111/j.1468-2427.2009.00899.x

Newell, B. C. (2018). Introduction. In B. C. Newell, T. Timan, & B.-J. Koops (Eds.), *Surveillance, privacy and public space* (pp. 1–15). Oxon: Routledge.

Newell, B. C., Timan, T., & Koops, B.-J. (Eds.). (2019). *Surveillance, privacy and public space*. Oxon: Routledge.

Nippert-Eng, C. (2010). *Islands of privacy*. Chicago: The University of Chicago Press.

Nissenbaum, H. (1997). Toward an approach to privacy in public: challenges of information technology. *Ethics & Behavior*, *7*(3), 207–219. Retrieved from https://nissenbaum.tech.cornell.edu/papers/toward_an_approach.pdf

Nissenbaum, H. (1998). Protecting privacy in an information age: the problem of privacy in public. *Law and Philosophy*, *17*(5/6), 559–596. Retrieved from https://www.jstor.org/stable/pdf/3505189.pdf?refreqid=excelsior%3A7c6ac63963d06a035b342ceb70d0562c

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(119), 119–158. https://doi.org/10.3868/s050-004-015-0003-8

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Nissenbaum, H., & Varnelis, K. (2012). Modulated cities: networked spaces, reconstituted subjects. *Situated Technologies Pamphlets 9*, 30. Retrieved from http://www.situatedtechnologies.net/files/ST9_ModulatedCities_web.pdf

Noor, S., & Metwally, L. (2018). *Hoe vergroot je het vertrouwen tussen jongeren en de politie?* Retrieved from https://www.kis.nl/sites/default/files/bestanden/Publicaties/vertrouwen-jongeren-politie_0.pdf

Norris, C. (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as social sorting: privacy, risk and digital discrimination* (pp. 249–281). Oxon: Routledge.

Norris, C. (2014). The success of failure: accounting for the global growth of CCTV. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 251–258). Oxon: Routledge.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: the rise of CCTV*. Oxford: Berg Publishers.

Nunnally, T. (2005). Explanatory Notes to Sigrid Undset, Kristin Lavransdatter (Part II, Ch. 2, note 1). In *The mistress of Husaby: Kristin Lavransdatter*. New York: NY: Penguin Books.

O'Reilly, K. (2009). *Key Concepts in Ethnography*. London: Sage publications.

Okin, S. M. (1989). *Justice, gender and the family*. New York: Basic Books.

Oldenburg, R. (1999). *The Great Good Place: Cafes, Coffee Shops, Bookstores, Bars, Hair Salons, and Other Hangouts at the Heart of a Community*. New York: NY: Marlowe & Company.

Olsen, F. E. (1983). The family and the market: a study of ideology and legal reform, *96*(7), 1497–1578.

Oravec, J. A. (2003). The transformation of privacy and anonymity, Beyond the 'right to be let alone.' *Sociologial Imagination*, *39*(1), 3–23.

Osucha, E. (2009). The Whiteness of Privacy: Race, Media, Law. *Camera Obscura*, *24*(1(70)), 67–107.

Packard, V. (1964). *The naked society*. New York: David McKay Company.

Pallot, M., Trousse, B., Senach, B., & Scapin, D. (2010). *Living Lab research landscape: from user centred design and user experience towards user cocreation*. Paris. Retrieved from https://hal.inria.fr/inria-00612632

Palmer, D., & Warren, I. (2014). The pursuit of exclusion through zonal banning. *Australian and New Zealand Journal of Criminology*, *47*(3), 429–446. https://doi.org/10.1177/0004865813514064

Pariser, E. (2012). *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. London: Penguin Books.

Park, R. E., & Burgess, E. W. (1921). *Introduction to the science of sociology*. Cambridge: Cambridge University Press.

Parkinson, J. R. (2012). *Democracy and public space: the physical sites of democratic performance*. Oxford: Oxford University Press.

Pateman, C. (1990). *The disorder of women: democracy, feminism and political theory*. Cambridge: Polity press.

Paton-Simpson, E. (2000). Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places. *The University of Toronto Law Journal*, *50*(3), 305–346. Retrieved from https://www.jstor.org/stable/pdf/825907.pdf

Patrikakis, C. Z., Kogias, D. G., Loukas, G., Filippoupolitis, A., Oliff, W., Rahman, S. S., … Elisabeth, Q. (2018). On the successful deployment of community policing services the TRILLION project case. In *2018 IEEE International conference on consumer electronics (ICCE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCE.2018.8326149

Patton, J. W. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology*, *2*(3), 181–187. Retrieved from http://www.riss.kr/link?id=O18099247

Patton, P. (1994). Metamorpho-Logic: Bodies and Powers in A Thousand Plateaus. *Journal of the British Society for Phenomenology*, *29*(2), 157–169.

Pedain, A. (2003). The Human Rights Dimension of the Diane Pretty Case. *The Cambridge Law Journal*, *62*(1), 181–206.

Periñán, B. (2012). The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law. *American Journal of Legal History*, *52*(2), 183–201.

Perrot, M. (1990). Introduction. In P. Ariès, G. Duby, & M. Perrot (Eds.), *A history of private life: from the fires of revolution to the Great War* (pp. 1–6). Cambridge: Massachusetts: The Belknap Press.

Petersen, J. K. (2012). *Handbook of surveillance technologies* (Third). Boca Raton: Florida: CRC Press.

Petronio, S. (2002). *Boundaries of privacy: dialectics of disclosure*. Albany: NY: State University of New York Press.

Pham, N., Ganti, R. K., Uddin, Y. S., Nath, S., & Abdelzaher, T. (2009). Privacy-Preserving Reconstruction of Multidimensional Data Maps in Vehicular Participatory Sensing. In J.

S. Silva, B. Krishnamachari, & F. Boavida (Eds.), *Wireless Sensor Networks. EWSN 2010. Lecture Notes in Computer Science, vol 5970* (pp. 114–130). Berlin: Springer Berlin Heidelberg.

Picard, É. (1999). The right to privacy in French law. In B. S. Markesisnis (Ed.), *Protecting privacy* (pp. 49–104). Oxford: Oxford University Press.

Pierson, J., & Lievens, B. (2005). Configuring Living Labs for a 'thick'' understanding of innovation.' *Ethnographic Praxis in Industry Conference Proceedings*, *2005*(1), 114–127. https://doi.org/10.1111/j.1559-8918.2005.tb00012.x

Poster, M. (1990). *The mode of information: poststructuralism and social context*. Cambridge: Polity press.

Proshansky, H. H., Fabian, A. K., & Kaminoff, R. (2014). Place-identity: physical world socialization of the self. In J. J. Gieseking & W. Mangold (Eds.), *The people, place, and space reader* (pp. 77–81). New York: Routledge.

Prosser, W. L. (1960). Privacy. *California Law Review*, *48*(3), 383–423.

Prost, A. (1991). Public and private spheres in France. In P. Ariès, G. Duby, & A. Prost (Eds.), *A history of private life: riddles of identity in modern times* (pp. 1–144). Cambridge: Massachusetts: The Belknap Press.

Puar, J. K. (2012). "I would rather be a cyborg than a goddess" Becoming-intersectional in assemblage theory. *PhiloSOPHIA*, *2*(1), 49–66.

Punter, J. V. (1990). The privatisation of the public realm. *Planning Practice and Research*, *5*(3), 9–16. https://doi.org/10.1080/02697459008722771

Rachels, J. (1984). Why privacy is important. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 290–299). Cambridge: Cambridge University Press.

Rachels, J., & Rachels, S. (2015). *The elements of moral philosophy* (Eighth). New York: McGraw-Hill.

Rainey, B., Wicks, E., & Ovey, C. (2017). *Jacobs, White, and Ovey: The European Convention on Human Rights* (Seventh). Oxford: Oxford University Press.

Ran, B., & Duimering, P. R. (2010). Conceptual Combination: Models, Theories and Controversies. *International Journal of Cognitive Linguistics*, *1*(1), 65–90.

Raz, J. (1986). *The morality of freedom*. Oxford: Oxford University Press.

Reamer Anderson, H. (2012). The mythical right to obscurity: a pragmatic defense of no privacy in public. *I/S: A Journal of Law and Policy for the Information Society*, *7*(3), 543–602. https://doi.org/10.3868/s050-004-015-0003-8

Records, computers and the rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. (1973). U.S. Department of Health, Education and Welfare.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: The University of North Carolina Press.

Regan, P. M. (2015). Privacy and the common good: revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: interdisciplinary perspectives* (pp. 50–70). Cambridge: Cambridge University Press.

Reidenberg, J. R. (2014). Privacy in Public. *University of Miami Law Review*, *69*(141), 141–160. Retrieved from http://ir.lawnet.fordham.edu/faculty_scholarship%0Ahttp://ir.lawnet.fordham.edu/faculty_scholarship/599

Reiman, J. H. (1984). Privacy, intimacy, and personhood. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 300–316). Cambridge: Cambridge University Press.

Reiman, J. H. (1995). Driving to the Panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, *11*(1). Retrieved from https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1174&context=chtlj

Reiter, E. H. (2009). Privacy and the Charter: Protection of People Or Places ? *Canadian Bar Review*, *88*(119), 119–146.

Richards, N. M. (2011). The limits of tort privacy. *Journal on Telecommunication and High Tech Law*, *9*, 357–384.

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*, *126*(7), 1934–1965. https://doi.org/10.1177/1753193411433524

Richards, N. M., & Hartzog, W. (2016). Taking trust seriously in privacy law. *Stanford Technology Law Review*, *19*(431), 431–463. https://doi.org/10.3868/s050-004-015-0003-8

Richardson, J. (2011). The changing meaning of privacy, identity and contemporary feminist philosophy. *Minds and Machines*, *21*(4), 517–532. https://doi.org/10.1007/s11023-011-9257-8

Richardson, J. (2016). *Law and the philosophy of privacy*. Oxon: Routledge.

Ricoeur, P. (1994). *Oneself as another*. Chicago: The University of Chicago Press.

Roberts, J. M. (2008). Publis spaces of dissent. *Sociology Compass*, *2*(2), 654–674.

Robins, K. (1995). Collective emotion and urban culture. In P. Healey, S. Cameron, S. Davoudi, S. Graham, & A. Madanipour (Eds.), *Managing cities: the new urban context* (pp. 45–62). Chichester: John Wiley.

Rodotà, S. (1974). La privacy tra individuo e collettività. *Politica Del Diritto*, *5*, 545–563.

Roessler, B. (2008). New ways of thinking about privacy. In J. S. Dryzek, B. Honig, & A. Phillips (Eds.), *The Oxford Handbook of Political Theory* (pp. 694–712). Oxford: Oxford University Press.

Roessler, B., & Mokrosinska, D. (2013). Privacy and social interaction. *Philosophy and Social Criticism*, *39*(8), 771–791. https://doi.org/10.1177/0191453713494968

Roessler, M. (2002). *How to find hidden cameras*. Retrieved from http://www.tentacle.franken.de/papers/hiddencams.pdf

Rohlf, D. (1980). *Der grundrechtliche Schutz der Privatsphäre: Zugleich ein Beitrag zur Dogmatik des Art. 2 Abs. 1 GG*. Berlin: Duncker & Humblot.

Romein, E., & Schuilenburg, M. (2008). Are you on the fast track? The rise of surveillant assemblages in a post-industrial age. *Architectural Theory Review*, *13*(3), 337–348.

Rose, G. (1993). *Feminism and geography: the limits of geographical knowledge*. Malden: Massachusetts: Polity press.

Rose, N. (1999). *Powers of freedom: reframing political thought*. Cambridge: Cambridge University Press.

Rössler, B. (2005). *The value of privacy*. Cambridge: Polity press.

Roßnagel, A., & Geminn, C. (2015). "Privatheit" und "Privatsphäre" aus der Perspektive des Rechts – ein Überblick. *Juristenzeitung*, *70*(14), 703–708.

Rothenberg, A. (1995). Creative cognitive processes in Kekulé's discovery of the structure of the benzene molecule. *The American Journal of Psychology*, *108*(3), 419–438.

Rouvroy, A., & Poullet, Y. (2009). The right to informational self-determination and the value of self-developments: reassessing the importance of privacy for democracy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 45–76). Dordrecht: Springer.

Rubinstein, I. S. (2018). Privacy localism. *Washington Law Review*, *93*(1961), 1961–2049. Retrieved from http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1853/93WLR1961.pdf

Ruddick, S. M. (1996). *Young and Homeless In Hollywood: Mapping the Social Imaginary*. New York: Routledge.

Rudinow, J. (1978). Manipulation. *Ethics*, *88*(4), 338–347.

Ruppert, E. S. (2006). Rights to Public Space: Regulatory Reconfigurations of Liberty. *Urban Geography*, *27*(3), 271–292.

Sadowski, J., & Pasquale, F. (2015). The spectrum of control: a social theory of the smart city. *First Monday*, *20*(7).

Sandel, M. (1982). *Liberalism and the Limits of Justice*. Cambridge: Cambridge University Press.

Scanlon, T. (1975). Thomson on privacy. *Philosophy & Public Affairs*, *4*(4), 315–322.

Schabas, W. A. (2017). *The European Convention on Human Rights: A Commentary*. Oxford: Oxford University Press.

Schachter, D. L. (2001). *The seven sins of memory: how the mind forgets and remembers*. Boston: Mariner Books.

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. In J. Domingue & E. Al. (Eds.), *The future internet* (pp. 431–446). Berlin: Springer. https://doi.org/10.1007/978-3-642-20898-0_31

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review*, *27*(1), 45–52. https://doi.org/10.1016/j.clsr.2010.11.009

Schliwa, G., & McCormick, K. (2016). Living labs: users, citizens and transitions. In J. Evans, A. Karvonen, & R. Raven (Eds.), *The experimental city* (pp. 163–178). New York: Routledge. Retrieved from http://lup.lub.lu.se/record/dd433415-5d8a-4879-b8ac-b45e557ee8fe

Schoeman, F. D. (1984). Privacy and intimate information. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 403–418). Cambridge: Cambridge University Press.

Schoeman, F. D. (1992). *Privacy and social freedom*. Cambridge: Cambridge University Press.

Schofield, P. (2009). *Bentham: a guide for the perplexed*. London: Continuum.

Schuilenburg, M. (2016). Predictive Policing : De Opkomst Van Een Gedachtenpolitie ? *Ars Aequi*, (december), 931–936.

Schuilenburg, M., & Peeters, R. (2015). From Biopolitics to Mindpolitics: Nudging in Safety and Security Management In From Biopolitics to Mindpolitics. *Culture of Control*, 1–7.

Schuilenburg, M., & Peeters, R. (2018). Smart cities and the architecture of security: pastoral power and the scripted design of public space. *City, Territory and Architecture*, *5*(1). https://doi.org/10.1186/s40410-018-0090-8

Schuurman, D., Mahr, D., De Marez, L., & Ballon, P. (2013). A fourfold typology of living labs: an empirical investigation amongst the ENoLL community. In *2013 International conference on engineering, technology and innovation (ICE) & IEEE international technology management conference* (pp. 1–11). IEEE. https://doi.org/10.1109/ITMC.2013.7352697

Schwartz, P. M., & Peifer, K.-N. (2010). Prosser' s "Privacy" and the German Right of Personality : Are Four Privacy Torts Better than One Unitary Concept ? *California Law Review*, *98*(6), 1925–1987.

Scott, J. (1990). *A Matter of Record: Documentary Sources in Social Research*. Cambridge: Polity press.

Scruton, R. (1987). Public space and the classical vernacular. In N. Glazer & M. Lilla (Eds.), *The public face of architecture: civic culture and public spaces* (pp. 13–25). New York: The Free Press.

Seligmann, L. J. (2014). Between Story Telling and Critical Analysis : Going Native and Crossing Borders. *Anthropology and Humanism*, *39*(1), 10–17. https://doi.org/10.1111/anhu.12032. Seligmann

Semple, J. (1987). Bentham's haunted house. *The Bentham Newsletter*, *11*, 35–44.

Sennett, R. (1992a). *The fall of public man*. New York: Norton.

Sennett, R. (1992b). *The uses of disorder: personal identity and city life*. New York: Norton.

Sharon, T., & Koops, B.-J. (2019). *Facial recognition and the ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces*.

Shelton, T., & Clark, J. (2016). Technocratic values and uneven development in the "smart city." Retrieved March 22, 2019, from https://www.metropolitiques.eu/Technocratic-Values-and-Uneven.html

Shelton, T., Zook, M., & Wiig, A. (2015). The "actually existing smart city." *Cambridge Journal of Regions, Economy and Society*, *8*(1), 13–25. https://doi.org/10.1093/cjres/rsu026

Shepard, M. (2011). *Sentient city: ubiquitous computing, architecture, and the future of urban space*. Cambridge: Massachusetts: MIT Press.

Shils, E. (1966). Privacy: Its Constitution and Vicissitudes. *Law and Contemporary Problems*, *31*(2), 281–306. https://doi.org/10.2307/1190672

Shoben, E. J., & Gagné, C. L. (1997). Thematic relations and the creation of combined concepts. In T. B. Ward, S. M. Smith, & J. Vaid (Eds.), *Creative thought: an investigation of conceptual structures and processes* (pp. 31–50). Washington, DC: American Psychological Association.

Sibley, K. (1988). Survey 13: Purification of Space. *Environment and Planning D: Society and Space*, *6*(4), 409–421.

Silver, H. (2014). Editorial: the centrality of public space. *City and Community*, *13*(1), 1–4. https://doi.org/10.1111/cico.12056

Silverstone, R. (1993). Domesticating the revolution: information and communication technologies and everyday life. *Aslib Proceedings*, *45*(9), 227–233. https://doi.org/10.1108/eb051328

Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review*, *135*(3), 707–746.

Simmel, A. (1971). Privacy is not an isolated freedom. In J. R. Pennock & J. W. Chapman (Eds.), *Privacy (Nomos XIII)* (pp. 71–87). New York: Atherton Press.

Simmel, G. (1964). *The sociology of Georg Simmel*. (K. H. Wolff, Ed.). New York: The Free Press.

Sloan, R. H., & Warner, R. (2015). The Harm in Merely Knowing: Privacy, Complicity, Surveillance, and the Self. *The Journal of Internet Law*, *19*(3).

Slobogin, C. (2002). Public privacy: camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, *72*, 213–315. https://doi.org/10.3868/s050-004-015-0003-8

Slobogin, C. (2016). Policing as administration. *University of Pennsylvania Law Review*, *165*(91), 91–152.

Slobogin, C. (2018). Legislative regulation of government surveillance. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of surveillance law* (pp. 597–622). Cambridge: Cambridge University Press.

Smolders, K. C. H. J., de Kort, Y. A. W., & Cluitmans, P. J. M. (2012). A higher illuminance induces alertness even during office hours: findings on subjective measures, task performance and heart rate measures. *Physiology & Behavior*, *107*(1), 7–16. https://doi.org/10.1016/J.PHYSBEH.2012.04.028

Soetanto, D. P., & van Geenhuizen, M. (2011). Social networks, university spin-off growth and promises of 'living labs''.' *Regional Science Policy & Practice*, *3*(3), 305–321. https://doi.org/10.1111/j.1757-7802.2011.01044.x

Soja, E. W. (1996). *Thirdspace: journeys to Los Angeles and other real-and-imagined places* (First). Malden: Massachusetts: Blackwell Publishers.

Soja, E. W. (2010). *Postmodern Geographies: The Reassertion of Space in Critical Social Theory*. London: Verso.

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.15779/Z382H8Q

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Solove, D. J. (2007). "I've Got Nothing To Hide" and other Misunderstandings. *San Diego Law Review*, *44*, 745–772.

Solove, D. J. (2008). *Understanding privacy*. Cambridge: Massachusetts: Harvard University Press.

Somers, M. R. (1994). The Narrative Constitution of Identity : A Relational and Network Approach. *Theory and Society*, *23*(5), 605–649.

Sommer, R. (1969). *Personal space: the behavioural basis of design*. Prentice-Hall.

Sorace, S. (2016). Trillion - INSPEC2T SAG/EEG Workshop. London. Retrieved from http://webcache.googleusercontent.com/search?q=cache:kXaBLWDrdAcJ:trillion-project.eng.it/documents/10197/0/TRILLION%2B-%2BLondon2.0.pptx+&cd=1&hl=en&ct=clnk&gl=nl&client=firefox-b-d

Sorace, S., Quercia, E., La Mattina, E., Patrikakis, C. Z., Bacon, L., Loukas, G., & Mackinnon, L. (2018). Serious games: an attractive approach to improve awareness. In G. Leventakis & M. R. Haberfeld (Eds.), *Community-oriented policing and technological innovations* (pp. 1–9). Cham: Springer International Publishing.

Sorkin, M. (1992a). Introduction: variations on a theme park. In M. Sorkin (Ed.), *Variations on a theme park: the new American city and the end of public space* (pp. xi–1). New York: Hill & Wang.

Sorkin, M. (Ed.). (1992b). *Variations on a theme park: the new American city and the end of public space*. New York: Hill & Wang.

Springer, S. (2011). Public Space as Emancipation: Meditations on Anarchism, Radical Democracy, Neoliberalism and Violence. *Antipode*, *43*(2), 525–562. https://doi.org/10.1111/j.1467-8330.2010.00827.x

Staeheli, L. A., & Mitchell, D. (2004). Spaces of public and private: locating politics. In C. Barnett & M. Low (Eds.), *Spaces of democracy: geographical perspectives on citizenship, participation and representation*. London: Sage publications.

Ståhlbröst, A. (2008). Forming future IT - The living lab way of user involvement. Lulea: Doctoral Thesis. Retrieved from http://www.diva-portal.org/smash/get/diva2:999816/FULLTEXT01.pdf

Starr, A., Fernandez, L. A., Amster, R., Wood, L. J., & Caro, M. J. (2008). The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology*, *31*(3), 251–270. https://doi.org/10.1007/s11133-008-9107-z

Steel, M., & Symes, M. (2005). The privatisation of public space? The American experience of business improvement districts and their relationship to local governance. *Local Government Studies*, *31*(3), 321–334. https://doi.org/10.1080/03003930500095152

Steeves, V. (2009). 11. Reclaiming the social value of privacy. *Lessons from the Identitiy Trail: Anonymity, Privacy and Identity in a Networked Society*, *1*(1), 191–208.

Steinbock, A. J. (1995). *Home and beyond: Generative Phenomenology after Husserl*. Evanston: IL: Northwestern University Press.

Stember, M. (1991). Advancing the social sciences through the interdisciplinary enterprise. *The Social Science Journal*, *28*(1), 1–14.

Strömholm, S. (1967). *Right of privacy and rights of the personality: a comparative survey*. Stockholm: P.A. Norstedt & Söners Förlag.

Susser, D., Roessler, B., & Nissenbaum, H. (2019). *Online Manipulation: Hidden Influences in a Digital World*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006

Taekke, J. (2011). Digital panopticism and organizational power. *Surveillance & Society*, *8*(4), 441–454.

Tally, R. T. J. (2013). *Spatiality*. Oxon: Routledge.

Taylor, C. (1997). *Philosophical arguments*. Cambridge: Massachusetts: Harvard University Press.

Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017a). *Group privacy: new challenges of data technologies*. Dordrecht: Springer.

Taylor, L., Floridi, L., & van der Sloot, B. (2017b). Introduction: a new perspective on privacy. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies* (pp. 1–12). Dordrecht: Springer.

Taylor, L. M., Hume, I. R., & Welsh, N. (2010). Labelling and self-esteem: the impact of using specific vs . generic labels labels. *Educational Psychology: An International Journal of Experimental*, *30*(2), 191–202. https://doi.org/10.1080/01443410903494478

Thagard, P. (1984). Conceptual combination and scientific discovery. In *PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association, Vol. 1* (pp. 3–12). The University of Chicago Press.

Thaler, R. D., & Sunstein, C. R. (2009). *Nudge: improving decisions about health, wealth, and happiness*. London: Penguin Books.

Thomson, J. J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *4*(4), 295–314.

Thrift, N. (2003). Space: the fundamental stuff of geography. *Space: The Fundamental Stuff of Human Geography*, 2009. https://doi.org/10.4135/9781446261965

Timan, T. (2013). *Changing landscapes of surveillance: emerging technologies and participatory surveillance in Dutch nightscapes*. University of Twente. Retrieved from https://ris.utwente.nl/ws/files/6059635/thesis_T_Timan.pdf

Timan, T., Galič, M., & Koops, B.-J. (2017). Surveillance theory and its implications for law. In R. Brownsword, E. Scotford, & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation, and Technology* (pp. 731–753). Oxford: Oxford University Press.

Timan, T., Newell, B. C., & Koops, B.-J. (2017a). Introduction. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in public space: conceptual and regulatory challenges* (pp. 1–17). Cheltenham: Edward Elgar Publishing.

Timan, T., Newell, B. C., & Koops, B.-J. (Eds.). (2017b). *Privacy in public space: conceptual and regulatory challenges*. Cheltenham: Edward Elgar Publishing.

Townsend, A. M. (2013). *Smart cities: big data, civic hackers, and the quest for a new utopia*. New York: W. W. Norton & Company.

Trochim, W. M. K., & Linton, R. (1986). Conceptualization for planning and evaluation. *Evaluation and Program Planning*, *9*(4), 289–308.

Trottier, D. (2018). Revisiting privacy in public spaces in the context of digital vigilantism. In B. C. Newell, T. Timan, & B.-J. Koops (Eds.), *Surveillance, privacy and public space* (pp. 141–156). Oxon: Routledge.

Tuan, Y.-F. (2001). *Space and place: the perspective of experience* (Eighth). Minneapolis: University of Minnesota Press.

Tyler, I. (2013). *Revolting Subjects: Social Abjection and Resistance in Neoliberal Britain*. London: Zed Books.

Valverde, M. (2008). Police, sovereignty, and law: Foucaultian reflections. In M. M. Dubber & M. Valverde (Eds.), *Police and the liberal state* (pp. 15–32). Stanford: Stanford University Press.

van Arensbergen, W. (2018, April). Proef met veiligheid-app in Eindhoven. *ED*. Retrieved from https://www.ed.nl/eindhoven/proef-met-veiligheid-app-in-eindhoven~a3478048/

van Bon, S. (2018). *Diversiteit uitgelicht: signalen van discriminatie, uitsluiting en maatschappelijke spanningen in Eindhoven*. Retrieved from http://radar.nl/file/2827857/RADAR+-+Diversiteit+uitgelicht.pdf

van der Leun, J. (2014). Etnisch profileren in Nederland: wat weten we nou echt? *Het Tijdschrift Voor de Politie*, (7), 23–28. Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/89936.pdf

van der Ploeg, I. (2003). Biometrics and the body as information: normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), *Surveillance as social sorting: privacy, risk and digital discrimination* (pp. 57–74). Oxon: Routledge.

van der Sloot, B. (2015). Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data." *Utrecht Journal of International and European Law*, *31*(80), 25–50. https://doi.org/10.5334/ujiel.cp

van Dijck, J., & Poell, T. (2015). Social Media and the Transformation of Public Space. *Social Media and Society*, *1*(2), 1–5. https://doi.org/10.1177/2056305115622482

van Doorn, B. (2018, August). Stratumseind 2.0: Big Brother kijkt niet alleen mee, maar beïnvloedt je ook. *Omroep Brabant*. Retrieved from https://www.omroepbrabant.nl/nieuws/2821879/Stratumseind-2-0-Big-Brother-kijkt-niet-alleen-mee-maar-beinvloedt-je-ook

Van Eijk, G. (2010). Exclusionary policies are not just about the "Neoliberal City": A critique of theories of urban revanchism and the case of Rotterdam. *International Journal of Urban and Regional Research*, *34*(4), 820–834. https://doi.org/10.1111/j.1468-2427.2010.00944.x

van Gerwen, E. (2013). *Stratumseind 2.0: plan van aanpak*. Eindhoven. Retrieved from https://eindhoven.raadsinformatie.nl/document/1047462/1/document

Van Gorp, B. (2007). The constructionist approach to framing: bringing culture back in. *Journal of Communication*, *57*(1), 60–78. https://doi.org/10.1111/j.1460-2466.2006.00329.x

Van Melik, R., Van Aalst, I., & Van Weesep, J. (2009a). The private sector and public space in Dutch city centres. *Cities*, *26*(4), 202–209. https://doi.org/10.1016/J.CITIES.2009.04.002

Van Melik, R., Van Aalst, I., & Van Weesep, J. (2009b). The private sector and public space in Dutch city centres. *Cities*, *26*(4), 202–209. https://doi.org/10.1016/j.cities.2009.04.002

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/J.GIQ.2016.06.004

Vanolo, A. (2014). Smartmentality: the smart city as disciplinary strategy. *Urban Studies*, *51*(5), 883–898. https://doi.org/10.1177/0042098013494427

Velu, J. (1973). The European Convention on Human Rights and the right to respect for private life, the home and communications. In A. H. Robertson (Ed.), *Privacy and human rightd* (pp. 12–128). Manchester: Manchester University Press.

Vermeulen, M. (2014). *SURVEILLE Deliverable D4.7 The scope of the right to private life in public places*. Retrieved from https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.7-The-scope-of-the-right-to-privacy-in-public-places.pdf

Vincent, D. (2015). *I Hope I Don't Intrude: Privacy and its Dilemmas in Nineteenth-Century Britain*. Oxford: Oxford University Press.

Vincent, D. (2016). *Privacy: a short history*. Cambridge: Polity press.

Vlassenrood, L. (Edit. . (2017). Becoming a Smart Society. Retrieved from http://141.138.193.31/~datastudio/api/wp-content/uploads/2018/05/DATAstudio_Becoming_A_Smart_Society_DEF.pdf

von Hippel, E. (1988). *The sources of innovation*. Oxford: Oxford University Press. Retrieved from http://web.mit.edu/evhippel/www-old/books/sources/SofI.pdf

von Hirsch, A., & Shearing, C. (1999). Exclusion from public space. In A. von Hirsch, D. Garland., & A. Wakefield (Eds.), *Ethical Perspectives in Situational Crime Prevention* (pp. 77–96). West Sussex: Hart Publishing.

von Hirsch, A., & Shearing, C. (2000). Exclusion from public space. In A. von Hirsch, D. Garland, & A. Wakefield (Eds.), *Ethical and Social Perspectives on Situational Crime Prevention* (pp. 77–96). Oxford: Hart Publishing.

von Hirsch, A., & Shearing, C. (2016). Exclusion from Public Space. *Ssrn*. https://doi.org/10.2139/ssrn.2799204

Vreugdenhil, H., Slinger, Ji., Thissen, W., & Rault, P. K. (2010). Pilot projects in water management. *Ecology and Society*, *15*(3).

Wakefield, A. (2000). Situational crime prevention in mass private property. In A. von Hirsch, D. Garland, & A. Wakefield (Eds.), *Ethical and Social Perspectives on Situational Crime Prevention* (pp. 125–146). Oxford: Hart Publishing.

Waldman, A. (2018). *Privacy as trust: information privacy for an information age*. Cambridge: Cambridge University Press.

Walzer, M. (1983). *Spheres Of Justice: A Defense Of Pluralism And Equality*. New York: Basic Books.

Walzer, M. (1986). Pleasures and Costs of Urbanity. *Dissent*, *33*, 470–475. Retrieved from https://www.dissentmagazine.org/pdfs/walzerurban.pdf

Ward, T. B., Smith, S. M., & Vaid, J. (1997). Conceptual structures and processes in creative thought. In T. B. Ward, S. M. Smith, & J. Vaid (Eds.), *Creative thought: an investigation of conceptual structures and processes* (pp. 1–30). Washington, DC: American Psychological Association.

Warf, B. (2011). Teaching time-space compression. *Journal of Geography in Higher Education*, *35*(2), 143–161. https://doi.org/10.1080/03098265.2010.523681

Warf, B., & Arias, S. (Eds.). (2009). *The spatial turn: interdisciplinary perspectives*. Oxon: Routledge.

Warren, C., & Laslett, B. (1980). Privacy and secrecy: A conceptual comparison. In S. Tefft (Ed.), *Secrecy: A cross-cultural perspective*. New York: Human Sciences Press.

Weaver, T. (2014). *The Privatization of Public Space: the New Enclosures*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2454138

Weber, M. (2017). *Methodology of social sciences*. (E. A. Shils & H. A. Finch, Eds.). New York: Routledge.

Weintraub, J. (1997). The theory and politics of the public/private distinction. In J. Weintraub & K. Kumar (Eds.), *Public and private in thought and practice: perspectives of a grand dichotomy* (pp. 1–42). Chicago: IL: The University of Chicago Press.

Welch, M. (2008). Foucault in a post-9/11 world: excursions into security, territory, population. In *Carceral NotebooksVolume 4, Discipline, Security and Beyond: Rethinking Michel Foucault's 1978 and 1979 College de France Lectures* (pp. 225–240). Chicago: IL. Retrieved from http://www.thecarceral.org/cn4_welch.pdf

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

Westin, A. F. (1984). The origins of modern claims to privacy. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: an anthology* (pp. 56–74). Cambridge: Cambridge University Press.

Whitaker, R. (1999). *The end of privacy: how total surveillance is becoming a reality*. New York: The New Press.

Whyte, W. H. (1988). *City: rediscovering the center*. New York: Doubleday.

Wiig, A. (2016). The empty rhetoric of the smart city: from digital inclusion to economic promotion in Philadelphia. *Urban Geography*, *37*(4), 535–553. https://doi.org/10.1080/02723638.2015.1065686

Williams, R. W. (2005). Politics and Self in the Age of Digital Re(pro)ducibility. *Fast Capitalism*, *1*(1), 1–44. Retrieved from http://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.htm

Williams, Raymond. (1983). *Keywords: a vocabulary of culture and society* (Revised). New York: Oxford University Press.

Williams, Robin, & Edge, D. (1996). The social shaping of technology. *Research Policy*, *25*(6), 865–899. https://doi.org/10.1016/0048-7333(96)00885-2

Willis, K. S. (2016). Sensing place - mobile and wireless technologies in urban space. In L. Frers & L. Meier (Eds.), *Encountering Urban Places: Visual and Material Performances in the City* (pp. 155–170). Oxon: Routledge.

Wilson, A. (1996). How We Find Ourselves: Identity Development and Two Spirit People. *Harvard Educational Review*, *66*(2), 303–318.

Wisniewski, E. J., & Love, B. C. (1998). Relations versus Properties in Conceptual Combination Edward. *Journal of Memory and Language*, *38*, 177–202.

Witte, N. (2003). *Privacy: Architecture in Support of Privacy Regulation A*. University of Cincinnati. Retrieved from https://etd.ohiolink.edu/!etd.send_file?accession=ucin1053701814&disposition=inline

Wood, A. W. (2014). Coercion, Manipulation, Exploitation. In C. Coons & M. Weber (Eds.), *Manipulation: Theory and Practice* (pp. 17–50). Oxford: Oxford University Press.

Wright, D., Gutworth, S., Friedewald, M., Vildjiounaite, E., & Punie, Y. (2008). *Safeguards in a world of ambient intelligence*. Dordrecht: Springer.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers and Technology*, *28*(3), 277–298. https://doi.org/10.1080/13600869.2014.913874

Yarwood, R., & Paasche, T. (2015). The Relational Geographies of Policing and Security. *Geography Compass*, *9*(6), 362–370. https://doi.org/10.1111/gec3.12216

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication and Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713

Young, I. M. (2000). *Inclusion and democracy*. Oxford: Oxford University Press.

Young, I. M. (2011). *Justice and the politics of difference* (Second). Princeton: New Jersey: Princeton University Press.

Young, J. (2007). *The Exclusive Society: Social Exclusion, Crime and Difference in Late Modernity*. London: Sage publications.

Zedner, L. (2009). *Security*. Oxon: Routledge.

Zelermyer, W. (1959). *Invasion of privacy*. Syracuse, NY: Syracuse University Press.

Zerubavel, E. (2006). *The Elephant in the Room: Silence and Denial in Everyday Life*. New York: Oxford University Press.

Zimmermann, R. (1996). *The law of obligations: Roman foundations of the civil tradition*. Oxford: Oxford University Press.

Zook, M. A., & Graham, M. (2007). Mapping DigiPlace: geocoded Internet data and the representation of place. *Environment and Planning B: Planning and Design*, *34*(3), 466–482. https://doi.org/10.1068/b3311

Zuboff, S. (2019). *The age of surveillance capitalism*. New York: Public Affairs.

Zukin, S. (1995). *The Cultures of Cities*. Malden: Massachusetts: Blackwell Publishers.

Online sources

ACLU. (2018). Community Control Over Police Surveillance (CCOPS) Model Bill. Retrieved March 31, 2019, from https://www.aclu.org/other/community-control-over-police-surveillance-ccops-model-bill.

Amazon physical retail locations. (n.d.). Retrieved March 21, 2019, from https://www.amazon.com/find-your-store/b/?node=17608448011.

Anonymous. (n.d.). Retrieved March 21, 2019, from https://www.merriam-webster.com/dictionary/anonymous.

Autoriteit Persoonsgegevens. (2016). Cameratoezicht - Beleidsregels. Retrieved from https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

Autoriteit Persoonsgegevens. (2018). AP informeert branche over norm camera's in reclamezuilen. Retrieved March 27, 2019, from https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera's-reclamezuilen#subtopic-1727.

Becoming a Smart Society Embassy of Data. (2018). Retrieved March 31, 2019, from https://destaatvaneindhoven.hetnieuweinstituut.nl/en/activities-0/embassy-data. Eindhoven. (2017).

Bohman, J. (2005). Critical Theory (Stanford Encyclopedia of Philosophy). Retrieved March 19, 2019, from https://plato.stanford.edu/entries/critical-theory/.

Cadwalladr, C. (2017, May 7). The great British Brexit robbery: how our democracy was hijacked. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Christiano, T. (2006). Democracy (Stanford Encyclopedia of Philosophy_. Retrieved March 25, 2019, from https://plato.stanford.edu/entries/democracy/.

City of Seattle's Surveillance Ordinance 125376. (2017). Retrieved March 31, 2091, from https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance.

Cromarty, H., & Strickland, P. (2018). Rough Sleepers and Anti-Social Behaviour (England). Retrieved from https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7836#fullreport.

Darlow, B. (2003). History of defamation. Retrieved March 25, 2019, from https://englishlegalhistory.wordpress.com/2013/10/18/history-of-defamation/.

de Graaf, P. (2015, November 23). Een biertje met Big Brother erbij op Stratumseind. De Volkskrant. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/een-biertje-met-big-brother-erbij-op-stratumseind~b3cc767c/.

Difference Between Sensors and Actuators. (2018). Retrieved March 31, 2019, from https://techdifferences.com/difference-between-sensors-and-actuators.html.

EIP-SCC. (n.d.). The European Innovation Partnership on Smart Cities and Communities (EIP-SCC). Retrieved March 19, 2019, from https://eu-smartcities.eu/.

Enschede (gemeente). (n.d.). SMART: Self-Motivated And Rewarded Travelling. Retrieved March 19, 2019, from https://www.smartintwente.nl/over-smart.

European Commission. (2011). Brainport region is the "smartest region of the world." Retrieved March 19, 2019, from https://ec.europa.eu/digital-single-market/en/news/brainport-region-smartest-region-world.

European Commission. (n.d.). Smart cities. Retrieved March 19, 2019, from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

European Network of Living Labs. (n.d.). Retrieved March 23, 2019, from https://enoll.org/.

Friedl v. Austria. (1992). Retrieved March 28, 2019, from https://www.menschenrechte.ac.at/orig/94_5/Friedl.pdf.

Garrett, B. L. (2015, August 4). The privatisation of cities' public spaces is escalating. It is time to take a stand. The Guardian. Retrieved from https://www.theguardian.com/cities/2015/aug/04/pops-privately-owned-public-space-cities-direct-action.

Gemeente Rotterdam. (2019). Vergunning B- en C-evenement. Retrieved March 31, 2019, from https://www.rotterdam.nl/loket/vergunning-b-en-c-evenement/.

Greenfield, P. (2018, March 26). The Cambridge Analytica files: the story so far. The Guardian. Retrieved from https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

Handeyside, H. (2015). Be careful with your face at airports. Retrieved March 19, 2019, from https://edition.cnn.com/2015/03/19/opinions/handeyside-tsa-spot-program/index.html.

Hildebrandt, M. (2019). Counting as a Human Being in the Era of Computational Law (COHUBICOL). Retrieved March 26, 2019, from https://www.cohubicol.com/.

Karantzoulidis, S. (2018). How Advancements in Thermal Camera Tech Are Heating Up Opportunities. Retrieved March 31, 2019, from https://www.securitysales.com/surveillance/advancements-thermal-camera-tech-opportunities/.

Lupker and others v. the Netherlands. (1992). Retrieved March 28, 2019, from http://echr.ketse.com/doc/18395.91-en-19921207/view/.

Moxham, L. (2018). Implementation of ECtHR judgments – What do the latest statistics tell us? Retrieved from https://strasbourgobservers.com/2018/07/27/implementation-of-ecthr-judgments-what-do-the-latest-statistics-tell-us/.

NL smart city strategy: the future of living. (2017). Retrieved March 19, 2019, from https://instituteforfutureofliving.org/wp-content/uploads/NL_Smart_City_Strategie_EN_LR.pdf.

Obscurity. (n.d.). Retrieved March 21, 2019, from https://www.merriam-webster.com/dictionary/obscure#h1.

Pieters, J. (2016, October). Dutch police excessively target ethnic minorities: report. NL Times. Retrieved from https://nltimes.nl/2016/10/03/dutch-police-excessively-target-ethnic-minorities-report.

Pieters, J. (2016, May 31). Driving while black: rapper stopped by Zwolle police for pricey car. NL Times. Retrieved from https://nltimes.nl/2016/05/31/driving-black-rapper-stopped-zwolle-police-pricey-car/.

Privacy International. (2017). Biometrics knows no borders, it must be subject to extreme vetting. Retrieved March 19, 2019, from https://medium.com/@privacyint/biometrics-knows-no-borders-it-must-be-subject-to-extreme-vetting-b13bf6420253.

Rahim, Z. (2018, October 15). Hungary brings in ban on rough sleeping. The Independent. Retrieved from https://www.independent.co.uk/news/world/europe/hungary-homeless-ban-viktor-orban-rough-sleeping-street-a8584401.html.

Seattle. (2017). Master list of surveillance technologies. Retrieved March 31, 2019, from https://www.seattle.gov/Documents/Departments/SeattleIT/Master-List-Surveillance-Technologies.pdf.

Smith, K. L. (2017, November). The Inconvenient Truth about Smart Cities. Scientific American. Retrieved from https://blogs.scientificamerican.com/observations/the-inconvenient-truth-about-smart-cities/.

Stratumseind Living Lab. (2019). Living Lab, Stratumseind 2.0. Retrieved March 19, 2019, from https://www.facebook.com/LivingLabStratumseind/.

Triangulum project. (n.d.). Retrieved March 23, 2019, from https://www.triangulum-project.eu/?page_id=2137.

Unity 3d model van Stratumseind. Retrieved March 31, 2019, from https://data.eindhoven.nl/explore/dataset/unity-3d-model-van-stratumseind/information/.

van Dijk, M. (2018). Stratumseind: de datastraat van Eindhoven. Retrieved from https://innovationorigins.com/nl/stratumseind-de-datastraat-van-eindhoven/.

van de Nieuwenhof, J. (2015). Een kijkje in het Lab van het Stratumseind. Retrieved March 23, 2019, from https://innovationorigins.com/nl/een-kijkje-in-het-lab-van-het-stratumseind/.

Vinotion. (2019). Living Lab, Stratumseind 2.0. Retrieved March 27, 2019, from https://www.facebook.com/LivingLabStratumseind/.

Warf, B. (2017). Time-space compression. Retrieved March 22, 2019, from http://www.oxfordbibliographies.com/view/document/obo-9780199874002/obo-9780199874002-0025.xml.