Crime Prevention and Detection Technologies in Smart Cities: Opportunities and Challenges

JULIAN LAUFS

Thesis submitted in partial fulfilment of
the requirements for the degree of
Doctor of Philosophy
in Security and Crime Science

Department of Security and Crime Science
University College London
2022

Student Declaration

I, Julian Laufs, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Julian Laufs

January 2022

Abstract

Over the past decades, rapid urbanisation has led many cities around the globe to experience new challenges ranging from increased waste and traffic to crime and insecurity. So-called 'smart cities' offer a solution to these problems, aiming to make city services more efficient and effective through the deployment and use of information and communication technologies (ICTs).

While the impact of this substantial transformation towards the creation of smart cities has been explored from a number of perspectives, the topic is still under-researched with regards to security and crime prevention in cities. This thesis seeks to address this gap. It explores the role smart city infrastructure can play for surveillance and discusses opportunities and challenges this presents for crime prevention and policing. Interdisciplinary in nature, it draws from both urban studies and the field of crime science, aiming to provide evidence-based recommendations for researchers and practitioners in both areas. The thesis takes a three-pronged approach. First, a systematic review examines smart city crime prevention programmes and interventions currently in use. More specifically, it focusses on the functions of different technologies and how they are currently conceptualised. Second, a series of expert interviews considers police and crime prevention professionals' knowledge, experience and use of crime prevention strategies related to smart city technology, focusing on their perceptions of challenges such as those related to public opposition. Third, an online experiment is used to test which factors may impact the social acceptability of smart surveillance technologies. Overall, the thesis develops knowledge, practically applicable for academics, policymakers, and practitioners, by identifying specific technological interventions, potential pitfalls and challenges in their implementation, and factors that impact their social acceptability.

Impact Statement

This thesis is highly interdisciplinary in nature, encompassing the diverse fields of surveillance studies, crime science, and urban studies. Consequently, it presents findings relevant to those researchers in these fields. The research presented in this thesis adds to the growing body of literature surrounding the use of smart city infrastructure for crime prevention and policing. More specifically, the findings contribute to a better understanding of the conceptualisation and functions of security technologies in smart cities, organisational pitfalls in the procurement and use of new technologies, and the predictors of their social acceptability.

Structuring the thesis in three distinct studies allowed for the timely publication and presentation of the results. Where possible, research findings were published in an openly accessible way, and datasets were made available for future replication. This approach was adopted to allow for other researchers to transparently replicate the studies and to maximise the impact of the findings in academia. In addition, the findings have been disseminated at several academic meetings and conferences. Taking a critical and self-reflective approach, this thesis points towards a number of avenues for further research.

In addition to the academic audience, the thesis is aimed at practitioners and policymakers, for whom it presents evidence-based policy recommendations. Unlike many previous studies that focus primarily on theoretical and philosophical issues, this thesis builds on consultations and interviews with experts in order to ensure the practical applicability of the findings. This approach ensured not only that the research output was relevant to those working in the field but also that the results could contribute to the policy discourse on the topic. Outside of academia, the findings have been discussed with officials at the German Federal Ministry of the Interior and the UK Home Office, as well as crime reduction practitioners in London.

Overall, this doctoral work has already, and will continue to impact the academic and professional debate of surveillance and crime prevention in smart cities. It enriches the scholarly discussion through a number of publications and aims to help practitioners to make decisions about the procurement, deployment, and use of smart security technologies in future urban spaces.

Acknowledgements

Before diving into the research that I have conducted over the past three years, I would be remiss if I did not thank the people who made all of this possible and who supported me in the process.

Firstly, I want to thank my supervisors Hervé Borrion and Ben Bradford. This project would not have been possible without your guidance and insights. From the countless comments and your help in navigating the academic world to your support in finding a job and the encouragement in the more trying moments, I appreciate everything you have done for me.

I also would like to thank Shane D. Johnson who as Director of the Dawes Centre for Future Crime supported this research with funding and resources, and who provided many valuable opportunities.

Over the past four years in London, I met many incredible people and I feel so lucky to have befriended some of them along the way. To my colleagues and friends at UCL, thank you for making this time so special and for being so supportive! Somaya, Mohammed, Martin, JL, the lads, and all of the others I appreciate all your support and friendship. While unfortunately I cannot list everyone here, I do have to mention three of the best people I have met in London. Anna, Ruth, and Andi, I feel so lucky to have gained you as friends and I look forward to seeing you all around the world.

All my friends in Germany, the PCU crew and the Philosophers, you guys are the best! Thank you for welcoming me back in Germany and for providing some much-needed distraction when times got tough.

Thank you to Roleda for always being there and supporting me especially during the last year and the hardships of COVID. With you even the most difficult moments felt like a breeze, and I cannot thank you enough for all you have done for me.

Last but certainly not least, I want to thank my incredible parents Dorothee and Norbert. I am forever grateful for all of the love and support I have received from you. You were always there to celebrate every little achievement along the way and knew how to build me up in moments when I needed it the most. Without you, none of this would have been possible which is why I dedicate this PhD to both of you.

TABLE OF CONTENTS

TABLES

Chapter One

Introduction

This doctoral thesis identifies and discusses the opportunities and challenges associated with the use of smart city infrastructure for crime prevention and policing. In particular, it focusses on surveillance technologies and their social acceptability. This topic is explored through three individual studies, each of which sheds light on a different aspect of the larger phenomenon of crime prevention and policing technologies in smart cities.

1.1. The Focus of this Thesis: Smart Cities and Surveillance

Over the past decades, rapid urbanisation has led many cities, both large and small, to experience new challenges ranging from increased waste and traffic to crime and insecurity (Ankitha, Nayana, Shravya, & Jain, 2017). The concept of the 'smart city' offers a solution to these problems through the deployment and use of information and communication technologies (ICTs) (Ismagilova, Hughes, Dwivedi, & Raman, 2019; Matos et al., 2019; Sutriadi, 2018). By gathering large quantities of data through sensors distributed in the urban environment, smart cities strive to be self-regulating systems that adapt to new challenges and citizens' needs in real-time, rather than passive and inflexible living space (Bettencourt, 2014; Kitchin, 2014).

The concept of 'smart cities' is, however, more complex as it tries to describe the overarching idea of a networked, intelligent, and liveable city of the future. At the same time, the prefix 'smart' has lost much of its meaning in a world that offers everything from smart phones and smart watches to smart lights and smart houses. Because of this, as well as the diversity of political and economic interests in urban space, finding a clear definition of 'smart city' can be challenging. Although the conceptualisations in the literature vary in focus, scope, and format, one common factor is the instrumental application of sophisticated ICTs. Often smart cities promise, for example, to be able to better manage and control the energy supply, the daily traffic volume, the supply and disposal of goods, as well as logistics solutions, while optimising urban management processes and saving resources (Hollands, 2008). Many authors see smart cities, however, not only as a new trend in urban planning and design but rather as a necessary answer to some fundamental and existential problems faced by humanity, first and foremost including the looming climate crisis (Bär, Ossewaarde, & van Gerven, 2020; García Fernández & Peek, 2020; Papa, Galderisi, Vigo Majello, & Saretta, 2015). The smartification of cities, that is the process of creating 'smart cities', is likely to be an irreversible trend which will become growingly important in the future and is bound to have a lasting impact on urban infrastructure (Libbe, 2014; Lobsiger-Kägi et al., 2016). Such a fundamental transformation will naturally bring both benefits and pressures and reshape most elements of urban life.

While the discourse surrounding smart cities and the future of urban space is quite diverse, questions of policing and crime prevention are often not discussed even though they are fundamental to safe and liveable (smart) cities (Altomare & Cartlett, 2017; Brayne, 2017; Van Zoonen, 2016). In many places around the globe smart city infrastructure is being deployed at rapid speeds and the body of academic research on the topic is growing, however, little empirical research exists on smart city technologies and their role in crime prevention (Meijer & Bolívar, 2016; Perry, 2013).

Even though it is not a substantial part of the current academic debate, smart cities will likely have a significant effect on policing and crime prevention. On the one hand, smart cities will create new demands such as increased cyber vulnerabilities, offending opportunities, and possibly entirely new crime types (Joh, 2019b; Kitchin & Dodge, 2017; Straube & Belina, 2018). On the other hand, they will provide opportunities to improve policing and crime prevention practices (Chiodi, 2016; Straube & Belina, 2018).

Already today, policing and crime prevention increasingly rely on technological solutions that especially in times of austerity not only offer higher detection and conviction rates but also improved resource management and efficiency (Aden, 2019; Rossler, 2019; von Lucke, 2020). The creation of smart cities promises to increase and even speed up this reliance on technological solutions. As such, smart cities may create benefits for policing and crime prevention in one of two main ways.

Firstly, building smart cities requires either the creation of new or the retrofitting of old urban infrastructure. This transformation process offers a wide range of opportunities to include crime prevention principles in the urban design (Ceccato, 2020b). Such an approach can be considered to be passive as it relies on crime prevention by reducing environmental precipitators rather than the active involvement of police or other government intervention.

Secondly, once created, smart cities depend in their very nature on the continuous and ubiquitous gathering of data through a variety of new sensors to recognise patterns in citizens' behaviours and improve city services accordingly (Rathore, Ahmad, Paul, & Rho, 2016). Surveillance of many different factors such as flows of people, traffic, air quality, or lighting is a key part of the smart city concept.

This wealth of gathered data allows for deeper insights into urban life and as such creates possibilities to improve current crime prevention and policing strategies. This move towards deeper insights and more finely grained data can be seen as a continuation of the 'big data revolution' (Brayne, 2017) and the struggle to improve hot spot policing by refining the quality and quantity of information used to produce data about geographical trends in crime (Ferguson, 2014).

Improvements may be made to existing approaches such as predictive policing (Sandhu & Fussey, 2021) or consist of entirely new technological solutions to contemporary or future problems, e.g., as seen in the introduction of body cams.

The underlying mechanism of monitoring urban processes and gathering data can be summarised under the umbrella of surveillance, which is a fundamental tenet of smart cities. As such, *surveillance-oriented technologies* will form a special focus of this thesis. This is further justified by the systematic review presented in Chapter 3 which finds that many traditional and smart security technologies fulfil surveillance functions in the urban environment.

At the same time, however, surveillance, especially for the purpose of policing and crime prevention, is a topic that has attracted much controversy. While China has deployed the most comprehensive surveillance system in the world (Burnay, 2019; Knockel, Crete-Nishihata, Ng, Senft, & Crandall, 2015; Leibold, 2020), which might actually fit the in surveillance studies often-cited Orwellian narrative, another picture dominates in the West. Especially since the Snowden revelations, many people have become increasingly sensitive to issues of large-scale (government) surveillance (Adams, Arias-Oliva, Palma, & Murata, 2017a; Adams, Hosell, & Murata, 2017b; Hintz & Dencik, 2016; Wilton, 2017).

Public resistance against the use of facial recognition technology in a private development in London King's Cross district (Sabbagh, 2019) and more recently the protests against the introduction of COVID-19 vaccination passes (Lukpat, 2021) have brought both projects to a halt. This shows that *public acceptability* can be a major challenge for the deployment of new surveillance measures and as such will be another special focus of this thesis.

The societal importance of these individual issues, separately and in combination, should not be underestimated and it is only bound to increase in the future. In addition, the topic ties in with many other important societal issues such as the policing crises of racial inequality and social justice which were amplified by the COVID-19 pandemic (Joh, 2021; White, Harris, Joseph-Salisbury, & Williams, 2021). While proponents suggest that new technologies can result in fairer policing (Capers, 2016), critics argue that it may only enhance inequalities (Neyroud &

Disley, 2008; Udoh, 2020). This once again highlights the relevance of the topic and the call for future-oriented research such as this thesis.

In light of these many large-scale societal problems, this thesis seeks to improve our understanding of potential opportunities and challenges arising from the use of smart city crime prevention and detection technologies, from a crime prevention perspective. In doing so, a special focus is placed on the use of surveillance-oriented security technologies (SOSTs) and their social acceptability. In order to contribute to the debate of the aforementioned issues, the thesis aims to develop practically applicable knowledge by identifying specific technological interventions, potential pitfalls and challenges in their implementation, and factors that impact their social acceptability.

1.2. Aim and Approach of This Thesis

In summary, this thesis is concerned with exploring the opportunities and challenges that arise from using smart city technologies for crime prevention and policing. The overarching research question of this thesis is:

> *What opportunities and challenges do the use of smart crime prevention and detection technologies create for policing and crime prevention?*

To comprehensively answer this question, this thesis explores three different aspects of the smart city - surveillance nexus, breaking the research question down into a series of sub-questions (see 1.3). Firstly, it explores the functions that security technologies fulfil in smart cities and how these functions have been conceptualised in the literature. Secondly, to complement this conceptual and theoretical view, the thesis considers police and crime prevention professionals' knowledge, experience and use of crime prevention strategies related to smart city technology, including a focus on their perceptions of challenges such as those related to public opposition. Here, a specific focus is placed on the current procurement and deployment processes for security technologies and the usefulness of new technologies for surveillance.

This focus on surveillance is also maintained in the last study, which takes a closer look at the issue of social acceptability. Through an online experiment, the thesis tests to what extent and why members of the public find the use of smart city technology for crime prevention more or less acceptable. The thesis analyses the factors that shape social acceptability of new security technologies both in terms of the characteristics of technologies themselves as well as the populations that are subjected to them.

Theoretically, the thesis is grounded in the literatures on smart cities and surveillance, recognising the reciprocal relationship between the two. It follows the notion that surveillance is both shaped by the environment within which it is placed, and at the same time shapes this environment (Kudlacek, 2015). As an interdisciplinary piece of work, this thesis falls neither fully in the realm of urban studies nor classical crime prevention or surveillance literature. Instead, it picks concepts and theories from both fields, drawing from studies on the effectiveness and use of surveillance technologies and applying them in the context of smart cities.

This thesis aims to provide valuable insights for anyone interested in understanding how the benefits that smart cities offer can be used for surveillance to prevent crimes and improve policing. It offers a unique perspective, covering conceptual and practical issues alike. The value of this thesis lies, however, not only in integrating issues of surveillance and crime prevention into the smart city discourse but also in the policy recommendations that are developed throughout. These recommendations aim to guide future policymaking for the creation of smart cities and the governance of urban security in future urban infrastructure.

1.3. Thesis Structure

This thesis is divided into seven chapters. As discussed before, the overarching research question of this thesis was then broken down into a series of sub-questions which were answered throughout Chapters 3-6. Each of these chapters contributes as a standalone study to the academic debate and, at the same time, explores the overall topic from a different perspective. The following provides a brief overview of the contributions of the individual chapters.

Chapter 2 reviews the academic literature and introduces key concepts and definitions that are relevant to this study, examining the two broad thematical areas that this thesis combines: surveillance and smart cities. It introduces the topics of surveillance and the smart city context, explaining both what the concepts mean in theory as well as how they are implemented in practice and their technical components. Lastly, the chapter brings together the two fields and discusses why surveillance in smart cities are a unique case worthy of scholarly attention. The chapter ends with a description of the gap in the literature and reiterating the aims of this thesis, setting the stage for the subsequent empirical chapters.

Chapter 3 offers a systematic review of the literature on security technologies for smart cities. While both crime prevention and smart cities are often discussed individually and the focus of growing debates, they are rarely brought together. The chapter focusses on the security technologies used in smart cities and discusses how these technologies are currently conceptualised in the academic literature, what smart technological interventions for crime prevention the literature identifies, and what functions smart security technologies fulfil compared to traditional ones. The research questions Chapter 3 aims to answer are:

a) How does the academic literature conceptualise security technologies for crime prevention in smart cities?

b) What smart security technologies have been documented in the literature?

c) To what extent do the functions of smart security technologies differ from those of traditional security technologies?

As such, Chapter 3 serves two purposes. Firstly, as a standalone study, it contributes to the academic debate by introducing a new categorisation for security technologies and their functions in smart cities. For this purpose, it merges two established frameworks, one with a focus on threat detection functions introduced by Borrion, Tripathi, Chen, and Moon (2014), and the other with a focus on crime prevention functions proposed by Ekblom and Hirschfield (2014).

Secondly, in the context of this thesis, the chapter has a somewhat exploratory character. By identifying and reviewing 121 security technologies for smart cities, and by contrasting their functions with those of more traditional interventions, the chapter helps to determine the focus of this thesis. Finding that many of the developed technologies are surveillance-oriented, the results set the direction for subsequent chapters.

As a method, the systematic review ensures a high standard of academic rigour and lays the groundwork for the subsequent chapters. The new classification developed in this chapter can help to group and compare interventions and to explore the distinct set of opportunities and challenges that they bring about. As such, it delivers a valuable addition to the conceptual landscape while aiming to give practitioners a tool to navigate the complex nexus that is surveillance and crime prevention in smart cities. This project phase was completed in May 2019, and the results were published in 'Sustainable Cities and Society' (Laufs, Borrion, & Bradford, 2020a).

Chapter 4 examines what opportunities and challenges practitioners in London face in the procurement, deployment, and use of new security technologies. The chapter is founded on the notion that adopting such technologies is not straightforward and depends upon the buy-in of senior management teams and users. The research questions Chapter 4 explores are:

d) What knowledge do practitioners working in the field of crime prevention and surveillance in London have about smart SOSTSs and smart city technology in general?

e) What opportunities for improving the effectiveness and efficiency of surveillance do practitioners identify in the use of smart city technology?

f) What challenges exist that hinder the implementation and use of smart SOSTSs in London?

g) To what extent is public opinion and social acceptability considered to be a limiting factor for implementing and using smart SOSTSs?

These questions are explored through twenty expert interviews conducted with practitioners in London between August 2019 and March 2020. As a standalone study, this part of the thesis adds the practitioner perspective to the current academic debate, advancing the understanding of issues faced in innovation processes and their management.

The chapter finds a variety of issues and challenges related to technological innovation for policing and crime prevention. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public-private partnerships, and public acceptability. While individual practitioners may have the expertise and willingness to unleash the full potential of surveillance and crime detection technologies, they are usually restrained by institutional rules or, in some cases, inefficiencies. In terms of the latter, this chapter especially highlights the negative impact of a lack of technical interoperability of different systems, missing inter- and intra-agency communication, and unclear guidelines and procedures. The findings reiterate many of the results from the first study and contribute to a richer picture of smart cities and the ongoing debates on their likely risks and benefits. The chapter adds a new perspective and highlights several ways to improve the current academic discourse The results of this study have been published in the 'International Journal of Police Science and Management' (Laufs & Borrion, 2021).

Chapters 5 and 6 both aim to identify predictors of the social acceptability of new surveillance technologies. While both chapters are based on data from the same survey, they have different analytical foci and take distinct approaches in their method. Chapter 5 explores the characteristics of the technology as possible predictors, focusing on the amount of gathered data (i.e., the intrusiveness), the level of automation of data collection and processing, the deployment location, and the predicted effectiveness in terms of crime reduction. As such, Chapter 5 aims to answer the question:

h) What characteristics of smart SOSTSs (intrusiveness, level of automation, effectiveness, location) predict how socially acceptable these systems are?

The study feeds into the social acceptability literature and, even though it is not its main focus, contributes to the knowledge base for designing socially acceptable interventions. In the context of this thesis, it provides insights into which characteristics are likely to influence social acceptability. This helps to highlight which factors practitioners should focus on when selecting and deploying new SOSTs in the context of smart cities. The policy recommendations that are created based on this chapter are complemented by the analysis in the subsequent chapter.

Chapter 6 focuses on the demographic factors and experiences of individuals with crime and the police as predictors of social acceptability. It explores the following questions:

i) To what extent do demographic factors such as age, gender, ethnicity, or political affiliation predict the social acceptability of smart SOSTSs?

j) To what extent do previous encounters with the police and victimisation experience (trust in the police, expectation of effectiveness, previous experience with the police) predict the level of social acceptability of smart SOSTSs?

While Chapter 5 relies on simple analysis of variance, Chapter 6 develops a structural equation model (SEM) to highlight the complexity of social acceptability and the mediating effect of trust in police and privacy concerns. Overall, the two chapters shed light on likely predictors of social acceptability for new SOSTs. The study especially highlights the importance of mediating factors such as trust in police and privacy concerns in the formation of technology acceptance. In addition to advancing the conceptual understanding and providing policy recommendations for the socially acceptable deployment of use of new SOSTs in smart cities, the study also provides ideas for research to further explore the topic. From this, a number of policy recommendations are developed, which are further elaborated in the ensuing discussion.

Chapter 7 revisits the main findings of Chapters 3,4,5 and 6, contextualising them under the themes of opportunities and challenges for surveillance presented by smart city environments. The chapter then synthesises recommendations for practitioners and policymakers, making an overall plea for more evidence-based and forward-looking policymaking in the field of surveillance and crime prevention. Lastly, the chapter follows the example by (Macnish, Wright, & Jiya, 2020) and presents two scenarios for the socially acceptable and privacy-oriented use of SOSTs in future smart cities, before discussing avenues for future research.

Table 1: Overview of the three individual studies, research questions, and methods

Study and research questions	Method and data
Chapter 3 - Security and the Smart City: A Systematic Review	
• How does the academic literature conceptualise security technologies for crime prevention in smart cities? • What smart security technologies have been documented in the literature? • To what extent do the functions of smart security technologies differ from those of traditional security technologies?	Systematic review of the literature with 121 included studies. Reviewing the literature of the past 10 years (2009-2018).
Chapter 4 - Technology and Innovation in Policing and Crime Prevention: Practitioner Perspectives from London	
• What knowledge do practitioners working with crime prevention or detection technologies in London have about using new crime prevention technologies? • What opportunities for improving the effectiveness and efficiency of crime prevention do practitioners identify in using new crime prevention technologies? • What challenges exist that hinder the implementation and use of new crime prevention technologies in London? • To what extent is public opinion and social acceptability considered to be a limiting factor for implementing and using new crime prevention technologies?	Expert interviews with 20 practitioners in London, conducted between August 2019 and March 2020
Chapters 5 and 6 – Exploring Social Acceptability	
• What characteristics of smart SOSTs (intrusiveness, level of automation, effectiveness, location) predict how socially acceptable these systems are? • To what extent do demographic factors such as age, gender, ethnicity, or political affiliation predict the social acceptability of new surveillance technology? • To what extent do previous encounters with the police and victimisation experience (trust in the police, expectation of effectiveness, previous experience with the police) predict the level of social acceptability of new surveillance technology?	A vignette-based online-survey with 1,440 participants was conducted from February to April 2021. The resulting data was analysed using ANOVA and structural equation modelling

1.4. Dissemination

1.4.1. Published Papers

Elements of this research have been published in the following research articles in peer-reviewed journals:

- Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. Sustainable cities and society, 55, 102023.
  DOI: https://doi.org/10.1016/j.scs.2020.102023
- Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. International Journal of Police Science & Management.
  DOI: https://doi.org/10.1177/14613557211064053

1.4.2. Presentations

The studies within this thesis have been disseminated at several academic conferences, including the LINCS Conference (Belfast, 2019) and the International Relations and Diplomacy in the Post-Pandemic World Conference (Cracow, 2021). In addition, results have been presented during invited talks at UCL, Malmö Universitet, the German Federal Ministry of the Interior, and the UK Home Office.

Chapter 2

Background: Surveillance and Smart Cities

2.1. Chapter Overview

This chapter introduces the theoretical underpinnings of this research, examining the two broad thematical areas that this thesis combines: surveillance for crime prevention and policing and smart cities. The literature on surveillance to date is diverse but at the same time highly fragmented. It includes both niche technical research that focuses on specific camera systems and their elements (see for example: de Diego, San Román, Montero, Conde, & Cabello, 2018; Desai, Ambre, Jakharia, & Sherkhane, 2018; Hu & Ni, 2018; Jayavadivel & Prabaharan, 2021; Rao, Sudheer, Sadhanala, Tibirisettti, & Muggulla, 2020; Singh, Patil, & Omkar, 2018; Sugaris, 2020) and broad philosophical or normative literature that explores the phenomenon of surveillance from a sociological perspective (see for example: Burnay, 2019; Galič, Timan, & Koops, 2017; Lyon, 2001, 2006; Norris & Armstrong, 2020; Thomas, Piza, Welsh, & Farrington, 2021; Thompson, McGill, Bunn, & Alexander, 2020; van Heek, Arning, & Ziefle, 2017). To avoid the pitfall of applying a too technical or too broad perspective, this study aims to bridge the gap between the two fields, discussing both the theoretical and philosophical foundations, as well as technical and practical considerations of surveillance in the smart city context. The first section provides an overview of what surveillance is, its theoretical and philosophical foundations, as well as an introduction to surveillance practice and its relevance to policing in the 21st century. It narrows down different forms of surveillance in more detail and presents typical deployment architectures.

The chapter introduces the smart city context, explaining both what is meant by the term 'smart city' in theory and how it has been implemented in practice. Here, the chapter highlights the relevance of this study once again, emphasising the importance of forward-looking research and policymaking in this field. It also focuses on the role of crime prevention and policing in the smart city, connecting the two themes and setting the stage for the following chapters. Lastly, the chapter brings together the two fields and discusses why surveillance in smart cities is a unique case worthy of scholarly attention. The chapter ends with a description of the gap in the literature and reiterating the aims of this thesis.

2.2. What is Surveillance?

The term 'surveillance' is often only associated with the context of crime prevention and policing, invoking images of towering CCTV cameras. Most surveillance, however, occurs in other contexts such as traffic management, healthcare, or taxation, where governments (or private companies) collect large amounts of data to track citizens' actions and compel them to act a certain way (Hempel & Bittner, 2007; Thompson et al., 2020). Often, this is necessary to ensure government services or society as a whole function. If health interventions are not monitored, pandemics may spread uncontrollably; if taxation is left up to the individual, most people would not pay. Thus, at first glance, surveillance for the purpose of preventing and deterring crimes is not much different. This, however, is where the context begins to matter. When examining the before-mentioned examples, most readers will recognise that there is a significant difference in the potential consequences in whether the police or a healthcare provider use their data (Bernal, 2016; Lyon, 2003).

Due to the various contexts in which it has been applied, the term 'surveillance' has a number of different meanings. Surveillance is a broad concept and can include issues ranging from healthcare to the enforcement of taxation or voter monitoring (Bennett, 2015). Here it is important to clarify that this research deals with government surveillance, more specifically, surveillance by security agencies and the police. In this context, surveillance is primarily linked to and justified by issues of crime prevention and national security (Reddick, Chatfield, & Jaramillo, 2015; Thompson et al., 2020). Especially in this realm, surveillance has become increasingly common and, in instances, almost a routine government activity over the past decades (Denemark, 2012). While this section only provides a short overview of the concept of surveillance, a more in-depth practical and philosophical discussion can be found in Campbell and Carlson (2002).

Most current definitions discuss surveillance as a form of reducing uncertainty (i.e. risk management) by increasing social control (Campbell & Carlson, 2002). This mechanism functions in two ways. Firstly, surveillance gathers information and provides better insights into the monitored situation (Campbell & Carlson, 2002). Secondly, it influences individuals' behaviour towards more predictability (e.g., citizens will be less likely to commit a crime if they are aware that they are being watched) (Campbell & Carlson, 2002). This means that surveillance and control are concerned with ordering around indices of risk rather than more comprehensive notions of 'soul training' as discussed by Foucault (Fussey, 2007). As a result, surveillance is either categorised as a solution to many modern problems or as a means of public and private bureaucracies to gain and exert control over societies and individuals (Armitage, 2013; Beniger, 2009; Edwards, 2005; Giddens, 1985; Haggerty & Ericson, 2005; Hier, 2011; Marx, 1998; Norris & Moran, 2016; Richards, 2012).

While the term 'surveillance' does not underlie one common definition and there is some debate about how and when it occurs (Bernal, 2016; Marx, 2015). Authors such as Trüdinger and Steckermeier (2017) for example suggest that surveillance constitutes 'the strategic collection of information and of data about citizens.' One important feature that many (especially older) definitions miss is that government surveillance can occur in offline and online environments and may involve the direct or indirect collection of data (the latter being done by third parties) (Thompson et al., 2020).

In most cases, governments justify increased surveillance with improvements to security, crime prevention, prosecution, or dealing with threats to national security (Thompson et al., 2020). Often, surveillance capabilities are expanded in the aftermath of significant crises such as terrorist attacks, when public opposition is reduced (Fussey, 2007). The literature suggests that technology originally legitimized in such a context (e.g., counterterrorism) may later also be used to police other 'ordinary crimes'. An example of this is the use of automated number plate recognition in London that is now being used to police London's congestion charge (Fussey, 2007). This process of the steady expansion of capabilities is often called 'surveillance creep' (Fussey, 2007).

Nonetheless, many people are opposed to increased surveillance and seek to avoid being subjected to it (Joh, 2013). While this may not be true in every case, Google search traffic for virtual private networks and internet privacy increases after many major surveillance scandals (Thompson et al., 2020). As this study is primarily focused on the physical realm of government surveillance rather than online activity, the following sections will discuss surveillance technologies in use today in the UK using the example of CCTV and exploring benefits, theoretical foundations, and issues. Even though the thesis is not exclusively focussed on CCTV, a focus on CCTV and related open street visual surveillance serve as a useful reference point with which to make comparisons about the functions and characteristics of other new forms of related technologies. As discussed before, the term 'SOSTs' is used here to describe all surveillance-oriented new technologies, including those with a focus on visual surveillance. The term thus highlights the focus on surveillance while drawing a link to other smart security technologies. Though a more nuanced disambiguation of different forms of surveillance technologies may add value to the debate, it is not within the scope of this thesis. Instead, the thesis gives concrete examples where necessary, using specific technology functions and configurations (see Chapters 5 and 6) to draw general conclusions about the acceptability and societal impact of new surveillance technologies.

This brief introduction already allows a glimpse at the broad diversity that can be found in the literature on surveillance, ranging from discussions of the philosophical roots and ethical implications of surveillance to highly technical publications. In the following, both aspects will be touched upon to explore what surveillance actually means and why it is so important today.

2.2.1. The Philosophy of Surveillance: Privacy vs. Security

The Surveillance Camera Commissioner's strategic vision emphasises that surveillance cameras should be deployed while 'respecting the individual's right to privacy' (Surveillance Camera Commissioner, 2017, p. 1). In light of such statements and to fully understand the issue of surveillance in today's world, it is necessary to briefly examine the philosophical foundations and to revisit the discussion of privacy vs. security.[1] Thus, what follows is a truly short excursion into the philosophy of surveillance and the underlying question of privacy vs. security.

Though this debate has faced much criticism and is in some regards outdated (see also 4.3.2.), it is nonetheless considered an important vehicle to illustrate the potential costs of new surveillance technologies. Issues associated with the privacy vs. security framing are important to acknowledge and are highlighted in the following section as well as Chapter 4. Despite these limitations, the debate still helps to demonstrate and emphasise surveillance harms. In the context of this thesis, it is used to focus the discussion on the often complex and diverse costs of surveillance. Because a nuanced discussion of the complex nature of surveillance harms goes far beyond the scope of this thesis, the general notion of privacy thus

[1] Especially in the more normative surveillance literature, a brief discussion of Foucault is common practice.

serves as a placeholder and is symbolic for the wider harms associated with the use of new SOSTs.

For the sake of brevity, this section limits itself to the most relevant concepts that offer insights with regards to this thesis, foregoing lengthy debates on the rise of surveillance or discussions of power and the role of modernity.[2]

The underlying idea of surveillance provided by the state is that human beings have a fundamental need for safety and security, which in today's complex world, they cannot provide for themselves as individuals (Nagenborg, 2005, p. 20). While our ancestors may have been able to fend off wild animals alone, this may be disproportionately harder or impossible with a complex modern threat. This is due to the changing nature of threats as they are becoming increasingly diverse and less immediate in nature[3]. As such, humans need a protective zone that enables us to make autonomous decisions (Nagenborg, 2005, p. 20). In the sense of Thomas Hobbes' social contract, the guarantee of security and order is the central task of the state (Newey, 2008, p. 144). This task requires the concentration of the means of power, i.e., authority, legitimacy, and the ability to act, in the hands of the state as the supreme authority to enable citizens not only to live safely but also to live freely.

The state is therefore obliged to maintain social order and to effectively protect citizens' rights to freedom, especially those of socially weak individuals and minority groups. Hobbes maintained that individuals would have to give up some freedoms for the benefit of the social contract, which would guarantee individual safety and security and as such would enable other individual rights that are not possible in a state of nature (Huemer, 2013). In the modern world, the preservation and

[2] For these discussions, see, for example, Lyon (2001) or Monahan (2006).

[3] An example of this is a terrorist attack which may affect individuals in a variety of ways from loss of life to economic or psychological impacts.

establishment of security in democratic constitutional states nonetheless places the state in a predicament as the guarantee of the state's security obligations inevitably entails to some extent restrictions of individual freedoms (Büllesfeld, 2002, p. 2; Huemer, 2013). Nonetheless, (liberal democratic) states are still obliged to uphold both liberties (including the right to privacy) and security equally.

While security always comes at the cost of civil liberties, the restriction of civil liberties does not necessarily equal more security. The key reason for this is that the state cannot guarantee absolute security even at the cost of a total loss of privacy, as the danger of crime can never be completely eliminated in a liberal society (Reuter, Geilen, & Gellert, 2016). At the same time, the question of security vs. freedom is not a zero-sum game, as technologies (or policies) may impact neither or both. Similarly, especially in the digital age, privacy and security are not mutually exclusive but might guarantee each other (see for example end-to-end encryption).

With regards to surveillance in the more traditional framing of the debate however, Foucault argues that surveillance is always opposed to freedom (Foucault, 1975; McCahill, 1998). Even though Foucault never dealt directly with video surveillance or other forms of information technology in the contemporary sense (Coleman & McCahill, 2010, p. 19), his works build the foundation of many philosophical discussions on modern surveillance. The most notable concepts stem from his reappraisal of Jeremy Bentham's Panopticon, through which he developed his theory of what he calls a ‘disciplinary society’ (Foucault, 1975).[4]

Foucault sees Bentham’s panoptic prison as an isolated system and an example of a ‘totally managed world’ (Eigenmann & Rieger-Ladich, 2010, p. 226). As such, the panopticon or any prison or psychiatric clinic can serve as a metaphor for such a managed world (Sarasin, 2016, p. 128). Foucault argues that the panopticon

[4] Similarly, Gilles Deleuze's work on the concepts of control and the 'society of control' is often discussed (Galič et al., 2017).

describes a form of power relations between the surveillant and the prisoners that can also be applied to modern societies (Fox, 1998; Power, 2011).

For Foucault there is no place outside the Panopticon. Accordingly, it is never the use of technical surveillance measures that creates the panopticon, but always the social conditions. However, it is conceivable that the network of surveillance is tightened by technical surveillance measures and that the freedom of the observed is (further) restricted by this. Ultimately, however, it should never be disregarded that the panopticon is operated by those who are enclosed within it. These ideas can also be translated to the case of smart city surveillance and the smart city in general. Here, various systems are used to monitor different aspects of life in the city. Through the interplay and connection of these different surveillance systems, regardless of their purpose, surveillance becomes an all-encompassing state and an underlying reality of daily life.

With regards to surveillance technologies, Foucault's ideas are especially important when discussing functions and deterrence effects (see Section 2.2.4.1). In Bentham's panopticon, there is a constant state of present but unverifiable surveillance (Galič et al., 2017), which makes clear how important knowledge about surveillance is for the observed. Only those who assume that they are being monitored would behave in the way that the observers (in the mind of the observed) expect of them to. Therefore, it is not the actual surveillance that is decisive, but the observed person's perception of the surveillance (Kietzmann & Angell, 2010).

Furthermore, the relationship between the supervisor and the observed in the panopticon is remarkably similar to the relationship between the observed in front of the camera and the observer behind the camera. The perception is one-sided, and the observer is interchangeable. Against the backdrop of these assumptions, it becomes clear why the discussion of surveillance in the literature is rarely neutral. As a result, especially in the literature in the relatively young field of surveillance studies, many contributions have a strongly normative character. One example of this is the frequent referencing of Lyon (2006), who argues that the structures behind surveillance demand a normative approach. The panopticon and the works of Foucault also build the foundation for many discussions of CCTV and technological surveillance tools in the broader context of surveillance and state control (Hier, 2011; Koskela, 2003; Rothe, 2003).

While supporters of surveillance at least historically often portray it as a magic bullet against crime and put internal security in the foreground, critics warn of the establishment of a surveillance state and the endangering of civil liberties (Lischka, 2017; Pavone, Santiago Gomez, & Jaquet-Chifelle, 2016; Töpfer, 2005). Even if one supports the (heavily simplified) argument that privacy is good and surveillance is, therefore, an evil, it is still difficult to argue effectively against those forms of surveillance that appear necessary to avoid a greater evil such as terrorist attacks (Reuter et al., 2016; Treibel, Korte, & Schäfers, 1997). Because this dilemma is so hard to solve, it is only possible to engage in a meaningful and practice-oriented discussion if surveillance is not considered to be evil per se and by asking under which conditions surveillance could be morally permissible. Some authors take the more measured approach of portraying security and privacy in terms of surveillance as a delicate balance (Sheldon, 2011). While taking part in the discussion is not the key aim of this thesis, the overall debate of security vs. privacy bears great importance as it underlies many modern discussions and provides a simplistic frame for discussion of the benefits and drawbacks of new systems.

2.2.2. Surveillance and Technology for Police in Practice

As the reception of surveillance technologies depends heavily on the national socio-cultural context in which they are deployed (Menichelli, 2014), the following section briefly recounts the history of surveillance technologies in the UK and the use by law enforcement over the years. While this thesis takes a diverse range of technologies into account, the historical account of surveillance is mostly focussed on CCTV, as it is the most commonly used technology.

2.2.2.1. History of Surveillance Technologies in the UK

While first video surveillance systems were developed as early as 1927 (Glinsky, 2000, pp. 46-47; Turtiainen, Costin, Hamalainen, & Lahtinen, 2020) and conventional video surveillance systems have their origins in the early 1940s (Krempel, 2016), Goold (2004) suggests looking back at the late 1980s and early 1990s to understand the history of CCTV in the UK.

The use of CCTV cameras in public spaces began in the UK as early as 1985 in Bournemouth. Eighteen cameras were installed in this tourist town to prevent vandalism on the beach and seafront, in a cooperative venture between local government and private interests (Gras, 2003, p. 30; McCahill & Norris, 2002). Up until then, CCTV had primarily been used in private businesses or used to regulate traffic. Although the British police used this image data in some cases, public police video surveillance only began with the project in Bournemouth. Today, more than 400 cameras monitor public space in Bournemouth (Gras, 2003, p. 30; McCahill & Norris, 2002).

By the end of the 1980s, several other towns around the country had adopted CCTV (McCahill & Norris, 2002; Norris & Armstrong, 1999, p. 80), but the rapid spread of the technology only really began when in 1994, the Conservative government included CCTV surveillance in its domestic security policy (Williams & Johnstone, 2000).

Between 1994 and 1998, the amount of CCTV cameras in British city centres quintupled (Gras, 2001). By 1998, 450 British cities and towns were already under CCTV surveillance (Gras, 2003, p. 30) and by 1999, the number of CCTV cameras in the UK was estimated to be between 200,000 and over one million with around 500 new CCTV cameras added every week (Büllesfeld, 2002, p. 35). Until the mid-1990s, CCTV systems, especially in urban centres, were heavily financed by the British government with the declared aim of tracking terrorist organisations such as the IRA and detecting and preventing planned attacks (Büllesfeld, 2002, p. 36). At the same time, however, studies show that despite falling crime rates, fear of crime was still relatively high in the UK population at the time, leading to a shift in the narrative and the increased use of CCTV as a tool to counter 'ordinary' crimes (Gras, 2003). Towards the end of the 1990s CCTV was primarily used for general crime prevention and detection in England and Wales. Today it seems to be indispensable as a policing tool in the UK (Büllesfeld, 2002, p. 36; Norris & Armstrong, 1999, p. 30), and most councils in the UK operate CCTV control rooms and surveillance infrastructure.

By 2002, the UK had the highest camera density in the world, with 95% of all English cities using CCTV cameras leading Norris and Armstrong to describe British citizens as the most surveilled in the world (Norris & Armstrong, 2016, p. 77). With little public opposition and legislation standing in the way, the meteoric rise of CCTV in the UK almost seems like an inevitable consequence of the gradual shift in thinking about crime and crime prevention (Hempel & Töpfer, 2002).

The extent of the popularity of CCTV as a key tool in crime prevention and detection become clear when examining the numbers. In the late 1990s, three-quarters of the entire Home Office crime prevention budget had been allocated to CCTV-related projects (Armitage, 2002), and the number of cameras skyrocketed over the past 30 years , with estimates today ranging from 4 to 5.9 million units in use (McCahill & Norris, 2003; Piza, Welsh, Farrington, & Thomas, 2019).

These estimates are, however, not uncontroversial and Gerrard and Thompson (2011) claim that these figures are grossly exaggerated and that the basis of these excessively high estimates is flawed. Instead, they find that it is much more likely that around 1,850,000 cameras are installed in the UK in 2011 and that a citizen is recorded on average by around 70 cameras per day (Gerrard & Thompson, 2011). Unfortunately, there are no reliable and current statistics on how many surveillance cameras are in use in the UK today that could serve to verify either number. Nevertheless, it is undisputed that the number of cameras installed in public spaces is steadily increasing and that over the past decades, most countries around the world have adopted CCTV as a central part of their crime prevention and public security efforts (Goold, 2004; Weisburd et al., 2019; Welsh & Farrington, 2009).

While in the early 2000s, the UK was still the biggest market for surveillance systems in Europe (Gras, 2003, p. 28), with one-fifth of all CCTV installations worldwide in the UK in 2004 (Coleman, 2012, p. 3), today this has changed. In 2016 the Surveillance Camera Commissioner warned in his annual report that public budget cuts were affecting CCTV, with systems being shut down and few new ones installed (Surveillance Camera Commissioner, 2016). This concern, however, has become less relevant over time with an increasing focus on smart technologies and growing enthusiasm to deploy smart surveillance systems. The National Surveillance Camera Strategy Objectives 2020-2023, for example, state the aim to explore future surveillance cameras as part of a 'broader integrated multi-sensor network and provide an evidence base for their deployment' (opportunities and challenges) (Surveillance Camera Commissioner, 2020).

Over the past decades, global trends have pushed the UK from its surveillance throne. China has expanded its public surveillance at rapid speeds over the past years, outmatching all other countries (Givens & Lam, 2019; Leibold, 2020; Zenz & Leibold, 2020) and more sophisticated systems using emerging technologies are being rolled out in cities such as Chicago, London, and Rio de Janeiro (Piza et al., 2019). This increased reliance on CCTV can, however, not only be observed internationally but also in local councils and communities in the UK (as shown in Chapter 4).

2.2.2.2. Beyond CCTV – The Dawn of New Technologies

The complex challenges that police face in the 21st century are often met with the deployment of new surveillance technologies, which some criticise as the use of technological fixes for social problems (Mitchener-Nissen, 2013). In light of this, it is imperative to contextualise CCTV in terms of technological innovation and to take a glimpse past the horizon of traditional camera-based surveillance systems (Skogan, 2019).

Increasingly fast-paced transnational crime and terror threats and heavily accelerated technological innovation have given rise to growingly complex surveillance technologies that have little in common with their predecessors (Bulut et al., 2009; Piza et al., 2019; Rasmussen, 2006). As such, the name 'closed-circuit television' seems today outdated as it in no way fits the description of modern surveillance technology. This notion is also discussed by other authors who suggest that neither the 'closed-circuit' nor the 'television' aspect are true for systems that can stream video and audio to any mobile device via the internet (La Vigne, Lowry, Markman, & Dwyer, 2011b).

Instead, the literature suggests terms such as the before-mentioned surveillance-oriented security technologies (SOSTs), which refers to all technological solutions aimed at detecting or preventing crime by gathering data and monitoring citizens, including traditional CCTV (Pavone & Esposti, 2012). While not all new security technologies are surveillance-oriented, the term is still useful as most new technologies for crime prevention and detection include some form of monitoring or sensing component (see Chapter 3).

While these new technologies provide a range of opportunities to improve surveillance and make systems more effective and efficient through the use of autonomous technologies and artificial intelligence (AI), they are also controversial. Especially their effectiveness depends on factors not immediately related to the technical specifications of the SOSTs themselves, such as the integration into the broader network and interplay with other smart city functions (Bier, 2012; Choi & Na, 2017).

These technological developments and the enabling of large-scale mass surveillance have heavily impacted the traditional triangle between privacy, public safety and technological developments (Mamonov & Koufaris, 2016) and have been criticised by many as the beginning of a 'brave new world' or the 'death of privacy' (Lauer, 2012; Nam, 2019).

2.2.3. SOSTs – Theory, Benefits, Criticism

Despite their growing popularity, there is still some debate about the benefits and upsides of using SOSTs to tackle crime. In the literature, there are several theoretical approaches that discuss how CCTV might affect crime, underpinning the use of SOSTs today. The following section will summarise these mechanisms and explore evidence for and against each case. While this section is aimed at discussing the theory, benefits, and criticism of SOSTs, CCTV is often mentioned throughout as it is the most frequently used and best researched example from the literature.

Authors such as Hefendehl and Stolle (2002) or Stierand (2000) have pointed out that there are three core functions of (video) surveillance. Firstly, SOSTs should contribute to the prevention of crime. Secondly, they should make it easier to solve crimes that have been committed, and thirdly, they should contribute to an improvement in the perception of security. While this categorisation is a good starting point for exploring the theoretical benefits of SOSTs, it only partially reflects the findings of other scholars. Most notably, these include Armitage (2002), who discusses CCTV and the mechanisms through which it functions in general and Tilley (1993), who discusses it in the specific context of theft in car parks. As such, the following will summarise the key mechanisms identified by Tilley (1993) and Armitage (2002), which can be clustered around three broad themes, surveillance as a deterrent, surveillance as a forensic tool, and surveillance as a tool to manage resources.

2.2.3.1. SOSTs as a Deterrent

While the literature suggests a number of different ways in which SOSTs can affect crime (Gill & Spriggs, 2005; Piza, Caplan, & Kennedy, 2014), its practical applications are often related to deterrence (Farrington, Gill, Waples, & Argomaniz, 2007; Ratcliffe, Taniguchi, & Taylor, 2009; Willis, Taylor, & Lee, 2017). Deterrence works (at least in theory) in a number of different ways, always relying on the underlying notion that the presence of SOSTs, and specifically CCTV, can lead to a higher likelihood for offenders to be 'caught, stopped, removed, [and] punished' (Tilley, 1993, p. 3). As such, it functions by increasing the (perceived) risk for the offender in order for them to choose not to offend if they suspect that they are being monitored (Sousa & Madensen, 2016). After interviewing 899 adult police detainees, Willis et al. (2017) come to the conclusion that CCTV is effective in reducing especially violent crime but less useful as a preventative measure. Most of the interviewed detainees were still likely to carry out the crimes regardless of CCTV, while using simple avoidance strategies.

While Tilley (1993) originally suggests that only a negligible number of arrests are made as a result of CCTV, more recent studies find that surveillance does, in fact, increase punishment on a case-to-case basis (Piza et al., 2014). This removal of the offender or at least the threat thereof is what this study calls 'direct deterrence'.

Using the terminology of Routine Activity Theory, Armitage (2002) suggests that CCTV may act as or at least imply the presence of a capable guardian (e.g., security personnel or police). While it is debatable to what extent a traditional CCTV system can be considered a capable guardian, smart systems may be more suitable to fill this role due to their capability to act (semi-) autonomously. SOSTs as a form of situational crime prevention rely thus on their ability to reduce or remove situational cues that rational choice and routine activity theory consider to be necessary prerequisites for crime to occur (Piza et al., 2019). The display of SOSTs aims to trigger a rational mechanism and change the situation in a way that the offender is ultimately dissuaded (Ratcliffe et al., 2009).

This, however, also means that the effectiveness of deterrence depends on the availability and readiness of other resources such as police or security officers (Tilley, 1993). If offenders see no risk of physical intervention, deterrence effects may be weakened. Other authors argue that this is not necessarily the case. Armitage (2002) compares this to Bentham's panopticon and the notion of power being visible but unverifiable, arguing that would-be offenders do not know whether police resources are available for intervention, and thus deterrence effects remain intact.

In addition to this direct deterrence effect, SOSTs can also have several indirect benefits. Because SOSTs may increase guardianship, citizens feel safer and more frequently use the area in question (Gill & Spriggs, 2005; McLean, Worden, & Kim, 2013; Spriggs, Argomaniz, Gill, & Bryan, 2005). Increased use of car parks, for example, might make drivers feel safer and thus increase traffic and natural surveillance (Tilley, 1993). Through this mechanism, SOSTs have shown to be, in some instances, a vital part in revitalisation efforts for crime-ridden and otherwise socially disadvantaged neighbourhoods (Klauser, 2007; Wheeler, 2016; Wiig, 2018). A caveat of this second function is, however, that it only applies to areas where (foot) traffic is possible. In addition, Graham, Brooks, and Heery (1995, p. 22) argue that 'by encouraging people to have faith in some disembodied electronic eye, CCTV may actually undermine the natural surveillance in towns and communities. (...) The result may be a further spiral of social fragmentation and atomisation, which leads to more alienation and even more crime.'

Furthermore, Tilley (1993) argues that the success and overall usefulness of CCTV always depend on the context. The study highlights that CCTV becomes especially effective when installed alongside other measures (raising credibility of threat) such as lighting, fencing, painting, visible security personnel, broadcasting of success (Tilley, 1993). This is further supported by research suggesting that the most effective surveillance systems are those integrated into wider police functions (Cameron, Kolodinski, May, & Williams, 2008; La Vigne et al., 2011b). Thus, instead of asking whether surveillance works in general, it is more sensible to ask under which conditions it works and how it can be used to address case-specific crimes (Tilley, 1993).

While this deterrence effect is often cited as one of the most noticeable effects of SOSTs, it is also criticised in the literature with several studies finding that offenders, especially those committing violent crimes, are in most cases not deterred by the presence of SOSTs (Butler, 2005; Ditton & Short, 1998; Ditton, Short, Phillips, Norris, & Armstrong, 1999; Gill & Spriggs, 2005; Gill & Turbin, 1998).

Other sociological and criminological analyses of video surveillance emphasise that SOSTs represent a form of situational crime prevention that is based on 'bad' incentive structures that make criminal activity rational (Garland, 2008, p. 291; Krasmann, 2004, p. 330). As discussed, surveillance is intended to show potential perpetrators that criminal offences will be sanctioned with a higher degree of probability and thus make criminal activity an irrational choice. While deterrence may be a strategy that works, the deterrence approach can have several negative effects, such as an increase in prison populations and the undermining of police-community relations (Tyler, 2021). Rejecting the notion that respect and obedience for the law depend largely on the threat of punishment, Tyler (2021) suggests that legitimacy is more important than deterrence in ensuring that individuals obey the law, emphasising that authorities need cooperation from the community to be effective in their work.

2.2.3.2. SOSTs as a Forensic and Investigative Tool

Another important function of SOSTs today is their use as a forensic and investigative tool. Compared to the literature on SOSTs as a deterrent or crime prevention tool, only little work exists exploring the use for investigative purposes (Ashby, 2017). Investigation or forensic use of SOSTs describes the gathering of evidence to ensure an increased rate of conviction for offenders and reduced ability to offend (through incarceration or increased supervision) (Armitage, 2002;

Brookman & Jones, 2021; Sousa & Madensen, 2016). SOSTs may help to answer the questions of the '5WH' formula5 of who, what, when, where, why and how (La Vigne, Lowry, Dwyer, & Markman, 2011a).

A key issue of using SOSTs as a tool for evidence gathering is, however, that their success depends highly on image or data quality and the placement of cameras and sensors (Henderson & Izquierdo, 2016; Ritchie et al., 2018) as well as the question of whether cameras or sensors exist at all (Ashby, 2017). Cameras that record low-quality footage may for example not produce admissible evidence and badly placed or somehow obscured cameras may not show the full scene, leading to a distorted picture of the situation. In many instances this means that the question is not whether the 5WH-questions can be answered but also whether the answer found through SOSTs is correct.

Results often depend on how cameras and sensors are installed and monitored (La Vigne et al., 2011b) and are contingent on the absence of so-called 'surveillance barriers' (Piza et al., 2014). Not only are technical specifications and the camera-to-operator ratio critical but the literature suggests that surveillance technologies may also produce unintended consequences such as crime displacement (Ratcliffe, 2006), increased fear of crime (Hempel & Bittner, 2007; Kazig, Frank, & Reiter, 2006; Reuband, 2001), and increased privacy concerns (Borrion et al., 2019; Sousa & Madensen, 2016).

This is further explored by Borrion et al. (2019) who discuss the unintended effects of crime prevention interventions in general, compiling a list that includes studies examining the economic impacts (Anderson, Chisholm, & Fuhr, 2009; Johnson, Tilley, & Bowers, 2015; Painter & Farrington, 2001; Roman & Farrell, 2002; Welsh & Rocque, 2014), social impacts (Clarke, 1997; Felson & Clarke, 2016; Norrie,

[5] For more information on the 5WH formula and its relevance for criminal investigations, see Stelfox (2013).

2002), and iatrogenic impacts (Braga, 2016; Cécile & Born, 2009; Dishion, McCord, & Poulin, 1999; Gatti, Tremblay, & Vitaro, 2009; Marx, 1995; Sherman, 2007; Weiss et al., 2005; Welsh & Rocque, 2014) of crime reduction measures. While most of these studies do not examine smart SOSTs specifically, they highlight the importance of holistic and interdisciplinary evaluations and the danger of severe unintended consequences due to the complex nature of crime prevention.

Lastly, using SOSTs for evidence gathering in criminal investigations can be problematic in terms of racial discrimination and procedural justice. While the data protection issues of video surveillance are often only discussed in political debates, a number of social science studies emphasise that video surveillance also leads to discrimination against certain groups of people (Lyon, 2003; Norris & Armstrong, 1999). As the evaluation of video recordings focuses (as done now) to a large extent on the external characteristics of a person, social prejudices regarding characteristics such as gender, skin colour, or clothing, are reproduced and solidified (Bier, 2012).Against this backdrop of (racial) discrimination, the removal of interpersonal or at least human components in law enforcement and surveillance through the deployment of smart SOSTs has been focus of positive expectation. Joh (2007), for example, speculates that such developments would 'render obsolete the litigation, public criticism, and academic critique' that has resulted from human enforcement practice.

In many instances, technological solutions for policing and crime prevention not only include evidence gathering capabilities but are also able to automatically deploy fines if punishable offenses have been recorded. With the spread of smart cities, this automation of enforcement processes and the integration with surveillance is likely to increase (Haggerty, 2004; Patterson, 2004; Seddon, 2004). Such systems offer cheap and reliable solutions especially suitable for non-violent volume crime and misdemeanours, circumventing lengthy bureaucratic and judicial processes (Seddon, 2004). At the same time, however, such systems require that complex situations are simplified into a dichotomy of punishable or permissible (Wells, 2008), effectively removing police discretion (Joh, 2007).

Many authors are, however, critical of the notion that AI and smart systems can be more objective than human analysts (Dienlin & Trepte, 2015; Garvie & Frankle, 2016; Lee, Quinn, & Pascalis, 2017; Lee, 2018; Noor, 2020). Critics find that in fact, a number of factors facilitate discrimination and bias based on ethnicity and gender by autonomous technologies (Noor, 2020). While in the case of traditional CCTV systems, the target selection can be hugely discriminatory towards certain groups of the population, depending on the bias of the operator, autonomous technologies may further enhance biases that are present in the data on which they have been trained (Lee, 2018; Noor, 2020). This may for example be the case if AI is trained on existing police databases that reflect existing racial biases and systemic injustices. This is a serious issue because when certain groups of individuals are disproportionately monitored, it unjustly criminalises them and conveys the larger societal message that they are not trusted (Armitage, 2002).

In addition, smart SOSTs, especially those with the build in function to sanction presumed offenders have severe implications for procedural justice (Wells, 2008). Even if smart SOSTs were able to avoid any build-in biases and fulfil some of the requirements of procedural justice such as 'consistency' (Lind & Tyler, 1988, p. 131), 'neutrality', 'lack of bias' (Tyler, 2021, p. 7) and 'impartiality' (Tyler, 2021, p. 117), there would still be severe shortcomings. This is due to the fact that procedurally just interventions also must be perceived as both 'respectful' and 'polite' to the individual involved (Tyler, 2021, p. 12). In addition, technological solutions must, further, contain 'opportunities to voice' (Lind & Tyler, 1988, pp. 170-172) where individuals can express their opinion or make their case, telling their 'side of the story' (Tyler, 2021, p. 194).

This is, however, often impossible, as the foundation of decision-making of automated systems is the dichotomy of punishable or permissible. The automation of decision-making furthermore creates black boxes which are bound to providing consistent results (Smith, 2020), but ignore notions such as 'common sense', 'discretion' and 'respect', which are generally considered vital to a 'just' experience or as Wells (2008) puts it: '[automated solutions] throw out the baby of respect for relevant difference with the bath water of prejudice.'

2.2.3.3. SOSTs to Manage Resources

Lastly, the use of surveillance technologies constitutes a foundation of modern policing paradigms such as intelligence-led policing which aims to change police practice away from reactive crime control toward proactive risk management (Manning, 2008; Sanders & Henderson, 2013; Sanders & Hannem, 2012; Sanders, Weston, & Schott, 2015). Intelligence-led policing also entails a focus on the 'primary means by which limited police resources can be deployed in a productive manner to better address community problems and ultimately reduce crime' (Taylor, Kowalyk, & Boba, 2007, p. 167). SOSTs can be valuable tools for police to ensure efficient resource deployment, i.e., cameras and other surveillance tools allow police to have a better overview over neighbourhoods or situations and deploy resources more efficiently (Tilley, 1993). This means that SOSTs are not directly used for the purpose of public safety, i.e., preventing crimes but rather the improved deployment of crime prevention resources and staff. A good example of this is the use of CCTV in railway networks, where it is primarily used for crowd management rather than investigation or prevention of crime (Ashby, 2017). Nevertheless, as a secondary function, the systems indirectly contribute to increased effectiveness of other crime prevention measures (Armitage, 2002; Ashby, 2017; Sousa & Madensen, 2016). Especially this function of surveillance systems may gain relevance in the smart city context as the smart urban environment relies on a multitude of sensors used for other primary functions, but which could deliver additional data to support policing.

In addition, SOSTs can provide ancillary benefits and improve police performance (Laufs, Bowers, Birks, & Johnson, 2020b; Sanders et al., 2015). CCTV and body cam footage can be used as evidence to corroborate crime reports, disprove claims of improper policing, increase conviction rates (Ariel, 2016; Fan, 2016, 2017; Morgan, 2013). Other surveillance tools such as the audio-based gunshot detection system ShotSpotter can help with the faster deployment of appropriate responses and allow police to gather intelligence and data on otherwise unreported incidents (Carr & Doleac, 2016; Germain, Douillet, & Dumoulin, 2011; Ratcliffe, 2006). In addition, the use of SOSTs in smart cities allows for the data gathering in previously unmonitored spaces. The monitoring of waste water for illicit drug residue can guide police for example to potential hot spots and provide valuable intelligence (Been, Esseiva, & Delémont, 2016; Kankaanpää, Ariniemi, Heinonen, Kuoppasalmi, & Gunnar, 2016). These functions allow not only to actively improve service effectiveness but also reduce what the literature calls 'failure demand', i.e., institutional inefficiencies often stemming from missing or incorrect information (Laufs et al., 2020b). Other evidence suggests that in some instances, arrests and direct police action were more likely when crimes were detected by CCTV rather than reported through calls for service (Piza et al., 2014). Police officials may thus be inclined to opt for CCTV if the performance of the force can be improved and resources can be spent more efficiently to manage police demand (Laufs et al., 2020b; Sousa & Madensen, 2016).

2.2.4. The Architecture of Different Surveillance Systems

CCTV and surveillance technologies for policing are not only being deployed in greater numbers but, as the previous sections point out, also becoming more technologically sophisticated with growing capabilities. While the systematic review in Chapter 3 discusses the functions of surveillance technologies in smart cities and smart surveillance in more detail, this section follows Sedky, Moniri, and Chibelushi (2005) who define requirements and introduce a classification for video surveillance systems. Their study defines three distinct categories of systems, including conventional, automated and smart video surveillance (Sedky et al., 2005). The transitions between the individual types of systems are fluid and cannot be defined by hard criteria. As such, the examples below are not exclusive, and variations of each system exist, but they help with a basic understanding of what surveillance means and how it looks in practice. The illustrations are based on the work of Krempel (2016) and serve to visualise the differences between the architectures.

2.2.4.1. Conventional Video Surveillance

The basic technical layers of the design of conventional video surveillance are presented in Figure 1. The aim of such a system is to enable a security guard to keep an eye on a larger area than would be possible without technology (Gill & Turbin, 1998). Cameras are used as sensors to visualise either distant areas or areas to which the view is limited by design. The infrastructure is typically based on analogue signal transmission. Proprietary methods are often used here, which makes systems from different manufacturers incompatible with each other. Modern conventional systems often include the ability to record video either on tape or digitally in order to retrace an event in retrospect. The video data from the cameras are displayed on monitor walls for the operator to evaluate. Simple control consoles allow the system to be switched on and off, access to an optional video archive and control any pan/tilt cameras that may be present. Today, most systems use IP cameras rather than ones that are individually wired to the processing unit.

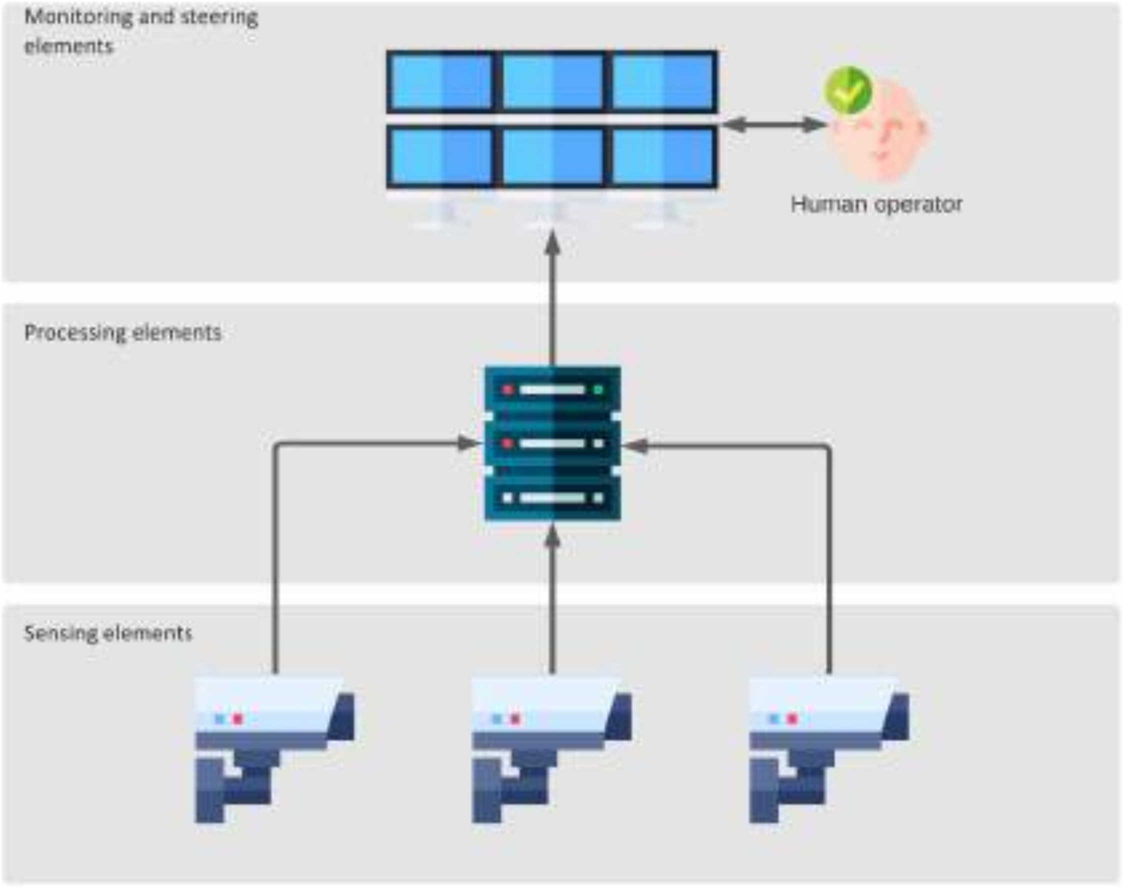


Figure 1 The components of a conventional video surveillance system (based on Krempel (2016))

2.2.4.2. Automated Surveillance

While many other studies only draw a distinction between conventional and smart surveillance systems, Sedky et al. (2005) introduce automated surveillance as an intermediate stage. Automated video surveillance systems try to reduce the operator's workload, or the storage needed for video archiving. Instead of simply showing the operator the live feeds from various cameras, automated systems try to draw attention to specific camera feeds or start recording automatically when a movement is detected. The methods used for image evaluation are, however, primitive as they are not able to capture the semantics of a scene. Most of these automated systems use simple motion sensors or movement detection mechanisms, but no distinction is made as to whether the camera records a person, cars or a branch moving in the wind.

The typical set-up of an automated video surveillance system can be seen in Figure 2. Automated systems use cameras as sensors and most of the systems already rely on digital infrastructure. They require additional infrastructure and processing capacity as well as more advanced cameras. Due to the increased standardisation of protocols and formats, components from different manufacturers can be combined to a limited extent. The operating devices are a mix of monitor walls, simple consoles, as in conventional systems, and commercially available PCs.

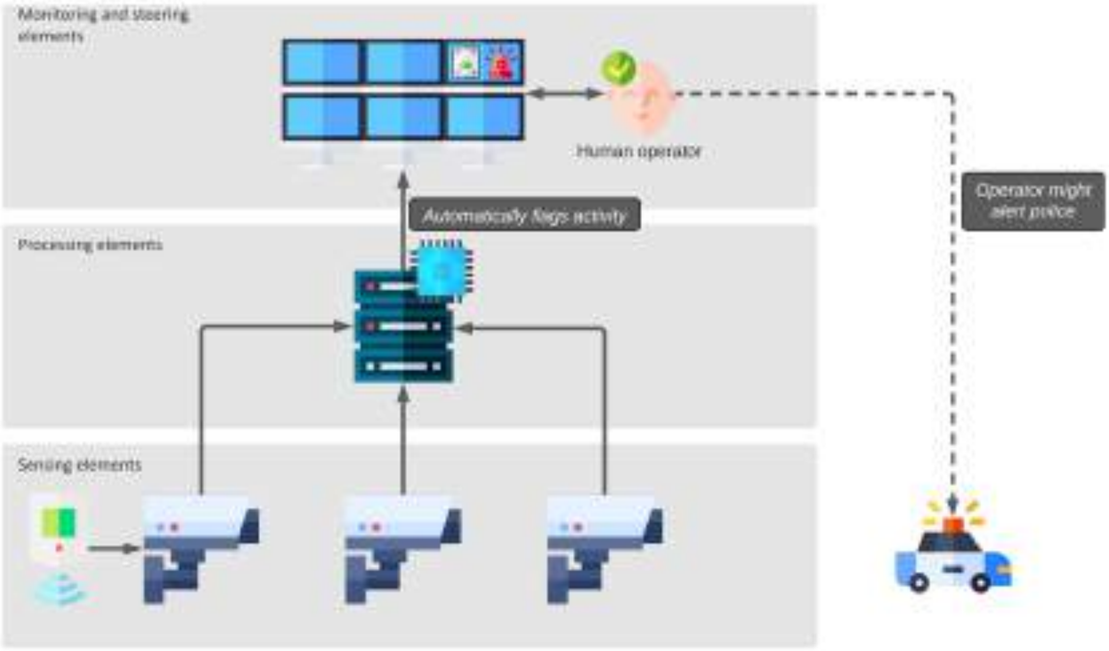

Monitoring and steering elements
Human operator
Automatically flags activity
Operator might alert police
Processing elements
Sensing elements

Figure 2 The components of an automated video surveillance system (based on Krempel (2016))

2.2.4.3. *Smart Surveillance*

In clear contrast to traditional, meaning both conventional and automated systems, smart surveillance systems are unique in three ways. Firstly, smart systems include additional components that cannot be found in conventional or automated systems. This includes additional sensing components that go beyond the use of cameras such as microphones (Benjamin, 2002; Gecas, 2016; Welsh & Roy, 2017; Zhao, Ma, Sun, Luo, & Mao, 2011) or radio frequency identification (RFID) readers (Haering, Venetianer, & Lipton, 2008; Saravanakumar, Deepa, & Kumar, 2017). Furthermore, processing can be done in either a centralised or decentralised manner (Desoi, 2018,

p. 35). In the case of the latter, at least some of the data processing and evaluation takes place in the individual sensor units while a larger processing unit compiles the pre-processed information for a complete picture. So-called smart cameras are increasingly being offered, which, in addition to pure recording, also take on initial evaluation tasks (Belbachir, 2010). Due to their three-dimensional recording of the environment, these cameras also allow complex sequences of actions to be recorded. Smart systems may also include both components that pre-process complex data and those that do not. In addition, smart systems do include not only additional sensors but also additional actuators that can be triggered in addition or instead of a police response. This includes for example the sounding of an alarm of the raising of lights (Al-Anbuky, 2014; Schuilenburg & Peeters, 2018). Figure 3 shows the typical technical structure of a system, where at least in theory, the high level of standardisation of all components allows components from different manufacturers to be combined with each other.

Secondly, due to the additional components and because smart surveillance is usually integrated in a wider network of sensors and actuators, smart systems have a range of further capabilities. Smart video surveillance uses image evaluation algorithms to assist the operator in evaluating the captured scenes. These algorithms are more powerful compared to automated systems and attempt to capture the semantics of a scene. Using algorithms and AI for video evaluation is a fundamental part of smart video surveillance (Hu & Ni, 2018).

It seeks to address the imbalance between the rapid increase of information and the lack of proper ways to analyse them, which might lead to problematic filtration and aggregation processes, which in turn may cause the overpolicing of certain societal groups (Fussey, 2007). As such, the aim of using these technologies is that operators do not have to recognise a critical situation by themselves but can rely on an algorithm to recognise it and then direct the operator's attention to it. Where currently many SOSTs only allow for the reactive deployment of police to incidents, smart systems seek to develop real time or even predictive capabilities (Catlett, Cesario, Talia, & Vinci, 2019; Degeling & Berendt, 2017; Macnish et al., 2020). While some research describes possibilities with which CCTV could become proactive through the use of AI (Bourmpos, Argyris, & Syvridis, 2014; Desai et al., 2018; Wiliem, Madasu, Boles, & Yarlagadda, 2012), others are more critical, finding that real-time interventions facilitated by surveillance are difficult to achieve (Fussey, 2007). In addition, Piza et al. (2014) emphasise that analysis capabilities need to scale with the deployment of sensors as lack of a proportional increase can become a barrier to efficient surveillance.

Scenes are evaluated in several steps and abstracted for further processing. Typical processing steps are the detection, classification and tracking of objects. Many systems also classify the behaviour of objects and can, for example, distinguish between different types of motion such as standing, walking, or running (Brezeale & Cook, 2008). Even though the development of algorithms for video evaluation is not part of this work and a deep technical understanding is not necessary, the following examples highlight the importance of algorithms and AI for modern surveillance and smart cities and aim to make the concept less abstract.[6]

Object detection forms the basis for almost all further algorithmic processing steps in video evaluation. Object detection algorithms are able to separate the relevant objects in the foreground from the background in an image or scene. By means of object classification, the objects recognised as relevant are assigned to different categories, such as person, car, or animal. Here, the video surveillance literature often discusses 'person detection' methods, which recognise objects in a scene and only process them further if they have been classified as human (Thys, Van Ranst, & Goedemé, 2019; Yang, Mahajan, Ghadiyaram, Nevatia, & Ramanathan, 2019).

[6] For an in-depth review of the current debate, see Hu, Tan, Wang, and Maybank (2004) and Wang (2013).

Object tracking is another process that aims to improve conventional video surveillance by tackling the issue of re-identification, i.e., identifying a person over a set of non-overlapping cameras in a multi-camera surveillance system (Almasawa, Elrefaei, & Moria, 2019; Byon, Kwon, Jung, & Lee, 2017; Wu et al., 2019). The particular challenge here lies in recognition of already known objects if they were (partially) no longer visible, for example, due to overlapping with other objects or because they entered a blind spot of the surveillance system (Almasawa et al., 2019). Re-identification processes can be divided into three classes: detection, recognition, and identification. Detection means that a video surveillance system is able to detect the object person in a scene. Recognition means that a video surveillance system recognises a person who has left the detection area of a camera and enters it again as the same person. Often the colour of clothing, gait or other soft biometric characteristics are used for recognition (Wu et al., 2019). If people leave the coverage area of all cameras for a longer period of time or change their clothing, they are typically no longer recognised. Lastly, identification is the highest level of person detection, where gathered data is compared to existing databases to find a person's identity using biometric facial data (Jayavadivel & Prabaharan, 2021). Recognition or identification are generally prerequisites for multi-camera tracking, as used in most smart surveillance systems.

Apart from the algorithms focused on (re-) identifying humans in the surveillance scenario, a number of other tools are important in the smart city case. These include the automated monitoring of pedestrian flows. This function becomes especially important for other city services such as traffic or public transportation management rather than policing (Akhter et al., 2019). Detecting large groups, estimating their size, and evaluating the direction of their movement is crucial to adapt services and ensure a smooth operation (Anees & Kumar, 2017).

In addition, behavioural analysis is necessary in smart cities, especially in the case of fully integrated systems such as the one shown in Figure 3. The algorithm is trained on distinguishing certain movement patterns to be able to recognise typical movements that could indicate issues such as violence (Nam, Alghoniemy, & Tewfik, 1998), the spraying of graffiti (Angiati, Gera, Piva, & Regazzoni, 2005), left luggage (Sacchi & Regazzoni, 2000) or the fall of a person (Tao, Turjo, Wong, Wang, & Tan, 2005). A special class of these algorithms tries to detect abnormal behaviour (Duque, Santos, & Cortez, 2007). This means that an algorithm learns the typical behaviour of people at a certain location and recognises when the current behaviour deviates strongly from this. With this class of algorithms, one tries to recognise events without being able to specify exactly what such events look like, such as an incipient panic. Similarly, other events that are unusual or break the pattern can be detected, e.g., fire or smoke (Liu & Ahuja, 2004).

Lastly, while conventional and automated systems require a human operator to take action to deploy a response, many smart systems include AI that can react to the gathered information autonomously. This is not to say that operators are entirely cut out of the process but rather means that human involvement is no longer necessary for a complete feedback loop between sensors and actuators. Today most smart surveillance systems are intended to support human operators in the detection and handling of security incidents. Especially in complex surveillance scenarios such as airports or city centres, that use a multitude of cameras and sensors, these systems are useful to bring order to the wealth of data. In addition, algorithms can at least to some extent compensate for human error as they do not get tired or distracted and deliver consistent results.

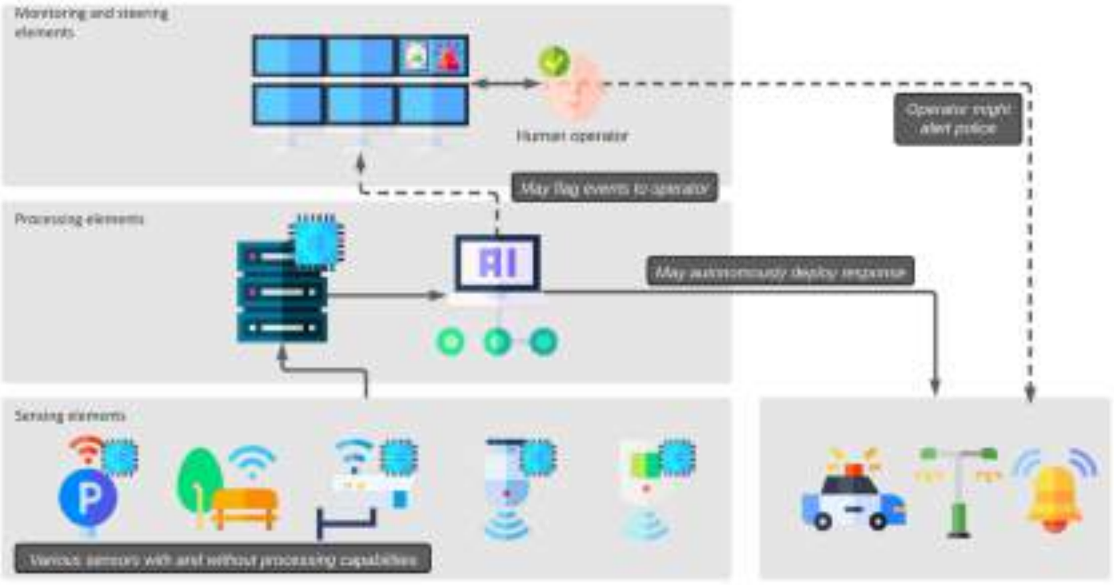

Monitoring and steering elements
Human operator
Operator might alert police
May flag events to operator
Processing elements
AI
May autonomously deploy response
Sensing elements
Various sensors with and without processing capabilities

Figure 3 The components of an intelligent video surveillance system (based on Krempel (2016))

2.3. What are Smart Cities?

The second half of this Chapter is devoted to the wider context of this thesis, namely the smart city. Before, however, delving into the technical aspects and necessary components of the smart city, a systematic approach to the term smart city is needed. In doing so, one inevitably encounters the fundamental difficulty of the smart city concept in the academic debate - the lack of a uniform definition. The attempt to find a definition is difficult, as many complex social and economic issues are embedded in the concept of the so-called 'smart city'.

There are, however, alternatives such as the conceptualisation introduced by Bayerl and Butot (2021) who follow Wittgenstein's (1953) concept of 'family resemblance' and discuss smart cities in terms of common universal components, namely technology, people, institutions, material environment. This allows for definitional flexibility and accounts for variations in the configuration of different smart city developments when empirically describing and assessing smart cities.

While the alternative conceptualisation by Bayerl and Butot (2021) is certainly innovative and useful for comparing or evaluating any specific smart city initiatives, it is not the most suitable for this thesis as smart cities are the contextual and overarching thematical frame and a static definition contributes to a more clear-cut picture.

As such, the following sections will introduce smart cities by briefly reviewing the definitions, underlying theoretical foundations, and by providing a context for crime prevention and surveillance in smart cities. This will help to illustrate the context of this thesis and set the scene for the subsequent empirical chapters.

2.3.1. Defining the 'Smart City'

In 2008, the world reached a tipping point, and for the first time in human history, the urban surpassed the rural population worldwide (Townsend, 2013). While especially Europe had long passed this point, with forecasts predicting 80% urban population in 2020 (Albino, Berardi, & Dangelico, 2015; United Nations, 2018), it was especially China's booming megacities and the exponentially growing urban developments in Africa that finally tipped the scales between urban and rural population (Townsend, 2013). The often-quoted prediction that more than 70% of the global population (or approximately 6.5 billion people) will live in cities by 2050 (United Nations, 2018) is almost symbolic for what authors call 'the biggest building boom humanity has ever undertaken' (Townsend, 2013).

This rapid urbanisation, however, brought and continues to bring about a long list of problems. The 'metabolism' of cities, i.e. the input of goods and the output of waste, is accelerated and amplifies environmental as well as social problems on an unprecedented scale (Albino et al., 2015; Marsal-Llacuna, 2016). This includes issues of waste, sewage, traffic, pollution, and noise – all of them often used as the poster child for negative consequences of this rapid urbanisation – are just the tip of the iceberg (Alirol, Getaz, Stoll, Chappuis, & Loutan, 2011; Berry, 2015). Instead, the before-mentioned urbanisation trends also cause social divide and reignite security issues, that were long believed to be solved (Chmutina & Bosher, 2017).

This rather dark picture of urbanisation is, however, not all there is to it. As people streamed towards the cities, technological developments accelerated, offering solutions to the these herculean challenges (Ankitha et al., 2017; Caragliu & Del Bo, 2018). The wide-spread proliferation of information and communication technologies (ICTs) in cities is today often considered one of the ways to deal with the challenges of inevitably growing urbanisation (Ankitha et al., 2017; Caragliu & Del Bo, 2018; Zhu, Li, & Feng, 2019). With this 'smartification' and the introduction of big data, a new trend was born, and with it, a broad array of questions as to their feasibility, and social and ethical acceptability.

Cities that use ICTs to solve urban problems are often referred to as ‘smart cities’. The concept first emerged in the 1990s (Alawadhi et al., 2012) as a technology-driven and solution-oriented alternative to traditional urban planning (Fernandez-Anez, Fernández-Güell, & Giffinger, 2018). Since then, governments and researchers have been decorating the word city with a variety of modifiers such as smart, intelligent, digital, knowledge, information, creative, or future (Gil-Garcia, Pardo, & Nam, 2015), using them as a marketing labels, or because it could help certain cities to distinguish and promote themselves as innovative and modern (Ramaprasad, Sánchez-Ortiz, & Syn, 2017). The discussion of what is the most fitting term has long taken off on its own and gotten detached from the original arguments. Liotine, Ramaprasad, and Syn (2016) for example consider the term smart city as an anthropomorphism (attribution of human characteristics to the city) because it is based on the ability of the city to sense and respond to its challenges smartly using natural and AI embedded in the city’s information systems. Hollands (2008) warns against the careless use of these labels altogether, as they are often used to describe (desired) innovation potential rather than concrete measures or characteristics.

While all of these labels more or less mean the same, attempting to describe some form of future image of city development, some put greater focus on technological aspects, while others pay more attention to the development of human capital or physical infrastructure (Chourabi et al., 2012; Gil-Garcia et al., 2015; Hollands, 2008; Nam & Pardo, 2011). This has often led to a convoluted discussion and a lack of definitional clarity. This is primarily due to the fact that because it is used so frequently and universally today, it can mean everything and nothing at the same time. Attempting to tackle this issue, many studies have attempted to define the smart city concept better, but because of its multidisciplinary nature, it is hard if not impossible to come to a single useful definition, and the question remains what a smart city actually is (Ramaprasad et al., 2017). Independently of or rather despite this lack of coherent conceptualisations, smart cities have become a dominant idea in urban management today (Bayerl & Butot, 2021).

While early attempts to lift the conceptual fog around the term focussed primarily on technology (Kummitha & Crutzen, 2017) and were largely concerned with the smartness in terms of information technologies for managing various city functions (Bakıcı, Almirall, & Wareham, 2013; Coe, Paquet, & Roy, 2001; Eger, 2009; Harrison et al., 2010; Lazaroiu & Roscia, 2012; Lombardi, Giordano, Farouh, & Yousef, 2012b; Mulligan & Olsson, 2013; Nam & Pardo, 2011; Townsend, 2013; Washburn et al., 2009), more recent attempts include a wider scope and consider the social dimension of sustainability, quality of life, and services to the citizens (Ahvenniemi, Huovila, Pinto-Seppä, & Airaksinen, 2017; Aloi et al., 2014; Anthopoulos, 2015; Bifulco, Tregua, Amitrano, & D'Auria, 2016; Hara, Nagao, Hannoe, & Nakamura, 2016; Herrschel, 2013; Huston, Rahimzad, & Parsa, 2015; Lee, Kim, Ryoo, & Shin, 2016; Lee & Lee, 2014; Marsal-Llacuna, 2016; Shapiro, 2006).

The latter in particular has led to further discussions with some authors such as Murgante and Borruso (2015) warning that the liberal use of this 'smart umbrella' often means that quick technological innovation is promoted at the cost of social and environmental factors. However, the widespread use of ICTs and the analysis of large amounts of data is a requirement for the 'smartness' of a city as it is the framework for sensing, monitoring, controlling and communicating between essential city services such as mobility and electricity networks, environmental and crime control, and social and emergency services (Akhras, 2000; Debnath, Chin, Haque, & Yuen, 2014; Murgante & Borruso, 2015).

Because not all cities are equally technologically advanced, studies have also stressed the need for objective measures to rank and categorise these developments according to variables such as economy, infrastructure, innovation, quality of life, resilience, transportation, and urban development (Giffinger & Haindlmaier, 2010). Before doing this, however, it is necessary to decide what should be considered a smart city and which elements such a system should include. To this extent, there have been many studies, often proposing a set of key components of a smart city and tools to assess the multiple capabilities of a city as it attempts to become smarter (Gil-Garcia et al., 2015). To address these issues for the comprehensive framework that is a smart city, it is necessary to take literature from a variety of different fields into account.

Ramaprasad et al. (2017) and Gil-Garcia et al. (2015) offer the most comprehensive overviews over the abundance of definitions found in the literature. While the former study finds more than 36 definitions of the term smart city and deconstructs them to create a single, unified definition, the latter study undertakes a comprehensive review of existing definitions and extensively explores different factors for ranking, evaluating, or guiding smart city efforts. For an overview, the table below summarises a variety of different definitions from the literature.

Table 2: Varying definitions of 'smart city' in the literature

Study	Definition
Bakıcı et al. (2013)	Smart city as a high-tech intensive and advanced city that connects people, information and city elements using new technologies in order to create a sustainable, greener city, competitive and innovative commerce, and an increased life quality.
Barrionuevo, Berrone, and Ricart (2012)	Being a smart city means using all available technology and resources in an intelligent and coordinated manner to develop urban centres that are at once integrated, habitable, and sustainable.
Caragliu and Del Bo (2018)	A city is smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance.
Chen, Fan, Xiong, Zhang, and Luo (2010)	Smart cities will take advantage of communications and sensor capabilities sewn into the cities' infrastructures to optimise electrical, transportation, and other logistical operations supporting daily life, thereby improving the quality of life for everyone.
Cretu (2012)	Two main streams of research ideas: 1) smart cities should do everything related to governance and economy using new thinking paradigms and 2) smart cities are all about networks of sensors, smart devices, real-time data, and ICT integration in every aspect of human life.
Eger (2009)	Smart community – a community which makes a conscious decision to aggressively deploy technology as a catalyst to solving its social and business needs – will undoubtedly focus on building its high-speed broadband infrastructures, but the real opportunity is in rebuilding and renewing a sense of place, and in the process a sense of civic pride. […] Smart communities are not, at their core, exercises in the deployment and use of technology, but in the promotion of economic development, job growth, and an increased quality of life. In other words, the technological propagation of smart communities is not an end in itself, but only a means to reinventing cities for a new economy and society with clear and compelling community benefit.
Giffinger, Fertner, Kramar, and Meijers (2007)	A city well performing in a forward-looking way in economy, people, governance, mobility, environment, and living, built on the smart combination of endowments and activities of self-decisive, independent, and aware citizens.

Guan (2012)	A smart city, according to ICLEI, is a city that is prepared to provide conditions for a healthy and happy community under the challenging conditions that global, environmental, economic and social trends may bring.
Hall et al. (2000)	A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, can better optimise its resources, plan its preventive maintenance activities, and monitor security aspects while maximising services to its citizens.
Harrison et al. (2010)	A city connecting the physical infrastructure, the IT infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city. […] Urban areas that exploit operational data, such as that arising from traffic congestion, power consumption statistics, and public safety events, to optimise the operation of city services.
Komninos (2006)	(Smart) cities as territories with high capacity for learning and innovation, which is built-in the creativity of their population, their institutions of knowledge creation, and their digital infrastructure for communication and knowledge management.
Kourtit and Nijkamp (2012)	Smart cities are the result of knowledge-intensive and creative strategies aiming at enhancing the socio-economic, ecological, logistic, and competitive performance of cities. Such smart cities are based on a promising mix of human capital (e.g., skilled labour force), infrastructural capital (e.g., high-tech communication facilities), social capital (e.g., intense and open network linkages) and entrepreneurial capital (e.g., creative and risk-taking business activities).
Kourtit, Nijkamp, and Arribas (2012)	The result of knowledge-intensive and creative strategies aiming at enhancing the socio-economic, ecological, logistic, and competitive performance of cities.
Lazaroiu and Roscia (2012)	A community of average size, technologically interconnected and sustainable, comfortable, attractive, and secure.
Lombardi et al. (2012b)	The application of information and communications technology (ICT) with their effects on human capital/education, social and relational capital, and environmental issues is often indicated by the notion of a smart city.
Marsal-Llacuna (2016)	Smart Cities initiatives try to improve urban performance by using data, information, and information technologies (IT) to provide more efficient services to citizens, to monitor and optimise existing infrastructure, to increase collaboration among different economic actors, and to encourage innovative business models in both the private and public sectors.

Nam and Pardo (2011)	A smart city infuses information into its physical infrastructure to improve conveniences, facilitate mobility, add efficiencies, conserve energy, improve the quality of air and water, identify problems, and fix them quickly, recover rapidly from disasters, collect data to make better decisions, deploy resources effectively, and share data to enable collaboration across entities and domains.
Thite (2011)	Creative or smart city experiments […] aimed at nurturing a creative economy through investment in quality of life which in turn attracts knowledge workers to live and work in smart cities. The nexus of competitive advantage has […] shifted to those regions that can generate, retain, and attract the best talent.
Thuzar (2011)	Smart cities of the future will need sustainable urban development policies where all residents, including the poor, can live well and the attraction of the towns and cities is preserved. […] Smart cities are cities that have a high quality of life; those that pursue sustainable economic development through investments in human and social capital, and traditional and modern communications infrastructure (transport and information communication technology); and manage natural resources through participatory policies. Smart cities should also be sustainable, converging economic, social, and environmental goals.
Toppeta (2010)	Combining ICT and Web 2.0 technology with other organisational, design and planning efforts to de-materialise and speed up bureaucratic processes and help to identify new, innovative solutions to city management complexity, in order to improve sustainability and liveability.
Washburn et al. (2009)	The use of Smart Computing technologies to make the critical infrastructure components and services of a city—which include city administration, education, healthcare, public safety, real estate, transportation, and utilities—more intelligent, interconnected, and efficient.
Woods and Goldstein (2014)	The integration of technology into a strategic approach to sustainability, citizen well-being, and economic development.
Zygiaris (2013)	A smart city is understood as a certain intellectual ability that addresses several innovative socio-technical and socio-economic aspects of growth. These aspects lead to smart city conceptions as 'green' referring to urban infrastructure for environment protection and reduction of CO2 emission, 'interconnected' related to revolution of broadband economy, 'intelligent' declaring the capacity to produce added value information from the processing of city's real-time data from sensors and activators, whereas the terms 'innovating', 'knowledge' cities interchangeably refer to the city's ability to raise innovation based on knowledgeable and creative human capital.

The conceptual maze surrounding the term smart city does, however, not stop with the question of which components a truly smart city needs but continues with issues of stakeholder management and governance. Especially in smart cities, these questions have gained renewed attention, as they are in many cases, unlike traditional urban spaces, not managed or owned publicly (Chourabi et al., 2012; Fernandez-Anez et al., 2018).

Thus, recent conceptualisations of smart cities have placed a larger focus on governance and the inclusion of stakeholders as key requirements for the success of smart city projects (Meijer & Bolívar, 2016). A commonly used model to understand the role of stakeholders in the smart city is the triple helix model (Deakin, 2014; Etzkowitz & Zhou, 2006; Lombardi et al., 2012a). The triple helix, originally a model to examine the interactions between academia, industry and governments, was first used by Leydesdorff and Deakin (2010) to explore the meta-stabilising potentials of urban technologies in Smart Cities. Building on this, Lombardi et al. (2012a) further developed the model to include civil society and Giffinger et al. (2007) finally suggested to add the dimensions of 'Governance', 'Economy', 'Environment', 'Mobility', 'People' and 'Living' as classification categories for smart city projects. These categories also reflect the recent trend of more citizen-centric approaches to smart cities (Castelnovo, Misuraca, & Savoldelli, 2016; Marsal-Llacuna, 2016).

Overall, the continuous evolution of the models reflects the growing focus on governance, the shift to more citizen-centric definitions and models (Castelnovo et al., 2016; Dameri, Negre, & Rosenthal-Sabroux, 2016; Fernández-Güell, Collado-Lara, Guzmán-Araña, & Fernández-Añez, 2016; Kummitha & Crutzen, 2017), and the key role assigned to the inclusion of stakeholders in more recent scholarship (Dameri, 2013; Fernández-Güell et al., 2016; Leydesdorff & Deakin, 2010; Lombardi et al., 2012a). At the same time, however, the large-scale use of ICT infrastructure in the context of smart city applications is often criticised for becoming dependent on private-sector interests or companies through close cooperation with large technology corporations, and for being increasingly shaped and driven by purely capitalist and market-based interests. The independent provision of infrastructure, according to Rötzer (2015, pp. 15-16), thus seems to be the crux of an independent smart city.

Which of the above-mentioned definitions one may pick, depends entirely on the nature of the project and the purpose the definition will serve. While some put the aim of the smart city in the foreground, others place a greater focus on the technological components (Albino et al., 2015). Alternative approaches exist that are for example more suitable for comparing different initiatives and analysing smart cities in terms of practices and outcomes, such as the one proposed by Bayerl and Butot (2021).

Aiming for a relatively parsimonious definition, this thesis answers the what, how, and why questions with the help of the above definitions in the following way:

> *A smart city is a city that uses information and communication technologies (ICTs) and all other technologies available to improve the effectiveness and efficiency of city services in order to save resources and to improve the quality of life for citizens.*

This definition includes both a focus on technological aspects as well as a specification of the broader aim, namely, to improve the quality of life for citizens. Adding this focus on the citizen is crucial because it will make it possible to go beyond the mere technological or ethical issues and explore issues of human welfare and social acceptability. The definition also deliberately states that 'all other technologies available' should be used because the term ICTs is today no longer sufficient to include most recent technological developments.

To conclude this discussion of the definitional issues surrounding the term smart city, a practical example is provided that highlights the different components that a smart city initiative can include. Bayerl and Butot (2021) group these components in four categories, technology, institutions, material environment, and people. Table 3 below presents the different components of the Stratumseind 2.0 project as identified by Bayerl and Butot (2021). The project is a smart city project in a nightlife area in Eindhoven, aimed at improving safety and liveability in the area by reducing aggression at night time. The example and the illustration in Table 3 show the centrality of ICTs but also emphasise the various other non-technological elements.

Table 3: Components of the Stratumseind 2.0 project adapted from Bayerl and Butot (2021)

Technology	Cameras for people counts, light sensors, wireless noise detectors, mac-address readers, social media web crawlers and sentiment analysis, data on mobile phone locations (purchased from providers)
Institutions	Local municipality, police, universities, businesses (bar owners, technology providers)
Material Environment	Street lighting, interactive displays on the street with visitor information (e.g., 'pub advisor')
People	Visitors, local inhabitants

2.3.2. The Importance of Security in the Smart City

So far, this chapter has discussed how the term 'smart city' has spread around the globe, affecting urban development programmes and government strategies (Berry, 2018). Many government initiatives seek to create a broad range of services, ranging from smart transport and smart energy to smart citizens and education (Hall et al., 2000). In addition, the previous section has laid out how smart cities are heralded for their efficient use of ICTs embedded within the fabric of urban environments that aim to improve and rationalise public services in the future (Berry, 2018). These futuristic scenarios, however, often fail to recognise safety and security as a focus (Hartama et al., 2017). This is critical, as it is not only one of the most basic tenets of urban planning and management but also of human wellbeing — after all, safety and security are on the second bottom layer of the Maslow pyramid (McLeod, 2007). As such, safety and security constitute factors that are integral parts of human well-being and as such also of any smart city design (Bourmpos et al., 2014; Reddy, Suresh, Phaneendra, Shin, & Odelu, 2018a)..

Only rarely does the literature acknowledge that rapid urbanisation leads to challenges for traditional safety and security infrastructure in cities (Isafiade & Bagula, 2017) and that these are critical issues for contemporary integrated urban developments (Benkő & Germán, 2016). Slowly, however, the realisation that crime and security problems are not isolated but often impact all other factors of city life, and as such should become a central issue in the creation of smart cities, has gained traction (Borrion et al., 2019).

One approach that aims to reconcile issues of crime prevention with new smart city developments is the safe city concept (Hartama et al., 2017). While initially conceived as a framework for safety for natural disasters, it quickly came to cover all aspects of safety within the city. In particular, the concept seeks to reconcile urban growth with the need for security through a variety of technological functions and by optimising the allocation of law enforcement resources (Castelli, Sormani, Trujillo, & Popovič, 2017; Oatley, Crick, & Bolt, 2015).

Integration may occur between individual algorithms such as those controlling sound recognition and lighting levels in parks, or between large infrastructures such as those managing water and electricity flows (Bayerl & Butot, 2021). Effectiveness and efficiency in smart cities, however, imply far more than only efficacy or financial concerns (i.e., whether the designated task has been completed and how much it costs). They also include issues of citizen satisfaction and whether the innovation has created a benefit to those subjected to the intervention and beyond. This is imperative, as citizens are in the end at the centre of any urban safety intervention and central to creating a safe environment (Cagliero et al., 2015). Thus, gauging the perceptions of citizens on urban security is a key point in Smart City management, as it will ensure that cities not only prevent or respond to safety risks and security threats but that they also remain an attractive place to live in (Cagliero et al., 2015).

2.3.3. Crime and Crime Prevention Dimensions of the Smart City

The displacement of essential services to the online realm and the installation of comprehensive smart systems leads to a sharp increase in (often sensitive) data being collected, stored and used (Ralko & Kumar, 2016). The promise of such large amounts of data, especially in an interconnected smart city system, extends to sectors such as (predictive) policing, surveillance, crowd control, or public sentiment monitoring (Van Zoonen, 2016). Thus, smart city technology creates a variety of opportunities for crime prevention. Luckily, issues of crime prevention and security are today in many instances no longer considered isolated issues but have long made their way into the sphere of public policy and urban planning. This form of comprehensive approaches can be clustered under the umbrella of so-called 'new crime prevention'(Chiodi, 2016). The concept of new crime prevention places a stronger focus on situational crime prevention (SCP) in the city (Beste, 2000; Selmini, 2004; Wurtzbacher, 2008).

The underlying assumption of SCP principles is that crime can be prevented, and opportunities for crime can be reduced by following a set of rules and by modifying situational precipitators that influence the offender (Clarke, 1995). The concept can neatly be summarised in five crime prevention or reduction methods, namely: increasing the effort to offend; increasing the risks of detection and apprehension; reducing the rewards for offending; reducing provocations that lead to offending; and removing excuses for offending, as perceived by offenders (Clarke, 1995; Cornish & Clarke, 2003; Noor, Nawawi, & Ghazali, 2013). Through these five principles, research on SCP has also significantly influenced Crime Prevention through Environmental Design (CPTED) (Cozens, Saville, & Hillier, 2005). CPTED aims to modify the physical and built environment to reduce the incidence and fear of crime (Crowe, 2000). Though including crime prevention principles into urban planning cannot single-handedly solve the problem of urban safety, it can nevertheless play an important role in influencing crime opportunities.

While it is expensive and impractical to retrofit cities according to the principles of CPTED, it is the development of smart cities that offers an unparalleled and untapped potential for crime prevention (WooChul & JoonYeop, 2017). Not only are smart cities by default constellations of instruments across many scales that are connected through multiple networks, providing continuous data regarding the movements of people and materials, but their development also often means changing and rebuilding the fundamental fabric of existing urban landscapes (Batty, 2013; Parra & Lopez, 2017).

2.3.3.1. SCP and CPTED in Smart Cities

Though traditional approaches to crime prevention in cities such as SCP or CPTED are widely accepted, their applicability to the increasing number of surveillance technologies used to prevent or detect crime in order to improve safety is debated (La Vigne et al., 2011b).

With regards to crime prevention in smart cities, principles of SCP and CPTED can be used to help decide how individual interventions should be designed and deployed. An example is the question of whether smart security measures should be constructed and deployed covertly or be made visible. While both options may have advantages, situational crime prevention principles advise that observable crime prevention measures are much more effective than those that are hidden from the public (and possible offenders) (Chiodi, 2016; Ekblom & Hirschfield, 2014).

Critics of these theoretical approaches argue, however, that while traditional crime prevention principles may still apply on some level and can add value to individual interventions, it is the emergence of smart cities and smart technology that compel a broader conceptualisation of the design of security, which has the potential to transform the governance of urban landscape so holistically (Benkő & Germán, 2016; Carter, Carter, & Dannenberg, 2003). Amongst many other concepts and ideas, Schuilenburg & Peeters (2018) propose to rethink the architecture of security in smart cities in terms of pastoral power, i.e. the governing of individuals and populations through care and protection (Slee, 2004) and once again reiterating the citizen-focus of smart cities (Boon, Malek, Hussain, & Tahir, 2017). Their concept, amongst many others, stands in contrast to traditional crime prevention approaches (e.g., SCP and defensible space), focussing on providing inclusive environments and providing 'scripts' for desirable behaviour in public space (Schuilenburg & Peeters, 2018).

Authors such as Schuilenburg & Peeters (2018) criticise aspects of traditional concepts such as SCP for their reliance on strategies of exclusion rather than through strategies to improve or strengthen what is already present (see also Breuil, Schuilenburg, & van Steden, 2014). In doing so, they raise important questions about the seemingly neutral strategies of SCP. A gated community, for example, may in many aspects fulfil all principles of SCP strategies, but it is the ethical dimension that raises serious questions about the fairness and universality of these measures (Duff & Marshall, 2000; Von Hirsch, Garland, & Wakefield, 2000). These issues are intensified in places such as malls where private stakeholders have the power to exclude specific individuals on non-criminal grounds (Wakefield, 2000). To avoid these pitfalls, Schuilenburg and Steden (2014) stress the need for urban safety and security through strategies based on positive attributes of living together (e.g., care, protection, belonging), grouped under the label of 'positive criminology' (Breuil et al., 2014; Gjørv, 2012; Schuilenburg & Steden, 2014). Taking this concept into account, it becomes clear that crime detection and prevention measures in smart cities can only guarantee an inclusive 'citizen focus' if they ensure equality (i.e., everyone is subjected to the same extent) and equity (i.e., no group is disproportionally affected by the outcomes) alike.

2.3.3.2. Crime Prevention and Sustainable Development

While some progress has been made and crime prevention is growingly considered as a part of public policy and social and urban planning, this is not always the case, especially with smart city developments (Chiodi, 2016; Cozens, 2002). In fact, many new urban planning and development strategies, especially for smart cities, stress sustainable development, i.e. 'development that meets the needs of the present without compromising the ability of future generations to meet their own needs' (WCED, 1987: 43), but ignore (or at least do not explicitly mention) aspects of security and crime prevention (Chiodi, 2016).

However, sustainable development and crime prevention are not mutually exclusive domains. Instead, several studies have linked CPTED directly with sustainable development in cities (Cozens, 2007; Cozens, 2002; Du Plessis, 1999; Henchley, Knights, & Pascoe, 2002). Neglecting crime as a factor thus means ignoring the important reciprocal relationship between crime prevention and sustainable development (Cozens & Davies, 2013). On the one hand, sustainable urban development can create socio-economic conditions that help prevent crime (Shapiro, 2006). As a variety of studies find, a comprehensive and inclusive approach to urban development can be a valid tool to combat urban decay and crime in a proactive way if underpinned by an interdisciplinary analysis of the urban fabric and specific local conditions (Cozens & Davies, 2013; Cozens et al., 2005).

On the other hand, safety from crime is an important condition for sustainable urban development and further smartification of cities (Ankitha et al., 2017; Crowe, 2000). Especially because safety from crime in an urban context is not only about the objective probability of becoming a victim of crime for citizens, but just as much about the perception of it, it is crucial to construct urban environments to give citizens a feeling of safety and prevent fear of crime (Baumer, 1978; Taylor, Gottfredson, & Brower, 1984). Feelings of security are important prerequisites for citizens' participation in the social and economic life of a city; they have outstanding importance for shaping city life and urban environments (Marshall et al., 2007; Smith & Clarke, 2000). In addition, participation may play a strategic role in any planning process that aims to create a safer city, and it is especially crucial to the effectiveness of CPTED (Sarkissian & Wenman, 2010). As such, preventing crimes and protecting citizens is not only an end in itself but also serves to support the wider smart city agenda of information technology-driven governance across various realms (Shelton, Zook, & Wiig, 2015; Wiig, 2018).

An example of this reciprocal relationship is the case of Camden, New Jersey. There, an integrated smart city strategy that fundamentally built on security and crime prevention components led to the revitalisation of the city (Wiig, 2018). The historically crime-plagued city tackled their issues with a data-driven policing strategy that allowed officers on the street to operate in tandem with a control room monitoring the city (Wheeler, 2016; Wiig, 2018). The success of this strategy meant not only that crime fell but also that other smart city initiatives in the realms of transportation and waste management could be realised, attracting further outside investment (Wiig, 2018). This in turn led to higher citizen engagement, the revitalisation of entire neighbourhoods, and more significantly falling crime numbers, even in areas that were not directly primarily affected by policing initiatives (Wiig, 2018).

This coupling of security — or at least the perception of it — with neoliberal urban revitalisation efforts, including the creation of new districts to attract multinational knowledge and innovation-focused industries, is at the heart of this security phenomenon (Cretu, 2012; Wiig, 2018). Smart security interventions are thus not the only part of the safety and security framework of the smart city but rather a puzzle piece in the bigger picture of innovative community policing strategies (Krivý, 2018).

However, this perspective is criticised heavily by authors who see it as a threat to the citizen-focus of smart cities (Cardullo & Kitchin, 2019; Mandl & Schaner, 2012).

Critics argue that while crime prevention and security measures in the smart city can be useful to pave the way for further smartification and the creation of a business-friendly city, they should not only be seen as such (Söderström, Paasche, & Klauser, 2014; Vanolo, 2014, 2016). Instead, authors such as Vanolo (2014, 2016) suggest that citizen welfare should not only be a pretence for underlying economic interests and the commercialisation of public spaces but rather a principle driver and in the spotlight of the smart city crime prevention debate.

While this may seem like an issue of semantics, several studies find that many smart city projects in cities like London or Dublin do not put the needs of their citizen in central position, but rather consider them passive beneficiaries (Boon et al., 2017; Cardullo & Kitchin, 2019; Willems, Van den Bergh, & Viaene, 2017). The citizen focus, also laid out in the definitions above, is especially necessary when discussing crime prevention and issues of safety and security in the smart city (van Heek, Aming, & Ziefle, 2016). This goes from the design of interventions to the deployment and issues of social acceptability.

2.3.3.3. Practical Issues of Crime Prevention in Smart Cities

In addition to these more normative questions, there are several practical considerations that have to be made when exploring crime prevention through smart technologies. Today, many issues of crime prevention are connected to the quality and availability of data. Several authors find that crime data often shows spatial and temporal inaccuracies (and omissions) which can have a great impact on the analyses and subsequent policy development (Harrell, 2014; Hart & Zandbergen, 2012; Johnson, Summers, & Pease, 2006). These vast inaccuracies can, to a large extent, be attributed to the slow and inaccurate processes to record spatial and temporal dimensions of crime (Mazeika & Summerton, 2017). While some authors suggest estimation techniques, e.g., using the earliest, latest, or average times that the crime could have occurred according to the victim, it is far from accurate and can severely impact crime data (Ashby & Bowers, 2013).

However, such inaccuracies are especially problematic in light of new technologies. Data mining, for example, is used to identify novel, implicit, and potentially useful information and patterns within the data and is a key tool in smart city designs (Schermer, 2011; Steinbock, 2005; Tien, 2004). As such, however, it relies on accurate information that can be accessed in real-time. This becomes especially clear when examining the literature on crime pattern theory. Angel (1968) suggests that robbery and other predatory offences are concentrated in "critical intensity zones' that, while being isolated, are situated in close proximity to busy locations, thus yielding a "spill over' effect. Other authors find that offenders follow their targets from busy to more isolated locations, where they perceive less risk (Summers & Johnson, 2017). While this highlights the role of data in contemporary crime prevention, it also provides a starting point for this project and for identifying possible shortcomings of today's crime prevention efforts in the UK.

In addition, the increased reliance on private interests and the management of parts of urban infrastructure through private rather than public providers might also pose a challenge to surveillance infrastructure and policing. As Ashby (2017) points out, no national registry of CCTV systems exists, meaning that police officers have to find out whether private CCTV exists and work to obtain the recordings. With the increasing reliance on private infrastructure and technology, this problem may be increased in the smart city environment, unless a fully integrated public-private network exists. The increasing privatization also contributes to the issue of 'black boxes' and the untransparent nature of algorithmic decision-making as many technologies are privately owned and proprietary, meaning they are unavailable for external scrutiny (Pasquale, 2015; Sandhu & Fussey, 2021).

Lastly, a significant change to the urban environment such as the one promised by the full smartification of cities will inevitably create new opportunities for crime (Berry, 2018; Truntsevsky, Lukiny, Sumachev, & Kopytova, 2018). In recent years, more and more studies have explored these new opportunities and crime types in the smart city, with a majority especially highlighting cyber offenses (see e.g., Baig et al., 2017; Chiodi, 2016; Elmaghraby & Losavio, 2014; Pelton & Singh, 2019). Even though this project primarily focuses on the built environment and as such disregards offenses that purely happen in cyberspace, crime type is not used to discriminate between interventions. Thus, new crime opportunities created through the use of smart interventions, will not be discussed further.

2.3.3.4. Military Urbanism and the Safe City

As shown in the previous sections, the link between security and smart urban developments is far from being free of controversy and has been the centre of much discussion. In the following, two concepts, the safe city concept and military urbanism, will be explored and their key premises and relevance for this thesis explained. They will help to provide an overarching theoretical framework and context with regards to basic tenets of security and smart cities.

The first concept is the safe city concept which puts security and crime prevention in the spotlight of urban development in order to improve city life and wellbeing of citizens (Mishra & Kumar, 2013). The approach aims to reconcile issues of security and crime prevention with new smart city developments (Hartama et al., 2017). While initially conceived as a framework for safety from natural disasters, it quickly came to cover all aspects of safety within the city. In particular, the concept seeks to reconcile urban growth with the need for security through a variety of technological functions and by optimising the allocation of law enforcement resources (Castelli et al., 2017; Oatley et al., 2015). Furthermore, a safe city describes integration of technology and the natural environment that 'enhances the effectiveness and efficiency of the process of handling the threat of crime and terror, to enable the availability of a healthy environment for citizens, and access to health, rapid response to emergencies' (Hartama et al., 2017). This definition is almost congruent with the general smart city definition introduced above but placing a greater focus on security and crime prevention aspects.

As discussed before, effectiveness and efficiency in smart cities imply far more than just operational or financial concerns (i.e., whether the designated task has been completed and how much it costs). They also include issues of citizen satisfaction and whether the innovation has created a benefit to those subjected to the intervention and beyond. As such, efficiency and effectiveness should in smart city context always be seen as part of a larger cost-benefit analysis. This is imperative, as citizens are in the end at the centre of any urban safety intervention and central to creating a safe environment (Cagliero et al., 2015). Thus, gauging the perceptions of citizens on urban security is a key point in Smart City management, as it will ensure that cities not only prevent or respond to safety risks and security threats but that they also remain an attractive place to live in (Caragliu & Del Bo, 2018). While emphasising the need for a citizen-focussed and human-centric approach, the safe city concept offers a generally positive outlook on security in smart cities and argues for an increased use of new security technologies to safeguard citizens and improve their wellbeing.

Other authors, such as Graham (2009) and Iveson (2010), see in the growing use of security technologies, and especially SOSTs, in smart cities, however, far more than just an attempt to better safeguard citizens and improve welfare. They discuss the developments as a militarisation of civil society by a state without an imminent security threat and rather as a translation of military ideas and security perceptions into the governance of urban civil society (Graham, 2004, 2013; Iveson, 2010). They see this 'urban militarism' as facilitated by a crossover between high-tech for civilian purposes and high-tech for military purposes with the aim to address pressing questions of both security and war in rapidly urbanising, globalised societies (Graham, 2004, 2005a, 2008).

Military urbanism sees the wide-scale use of security technologies as a (more or less subtle) continuation of war as a perpetual and boundless condition of urban societies, e.g., against drugs, against crime, and against terror. The concept warns of a creeping process of securitisation through the introduction of military ideas into the heart of everyday urban life (Graham, 2008; Salter, 2014). While military urbanism may seem like a rather extreme position at first, it, in fact, stresses democratic oversight and places similar to the safe city concept a large focus on citizen welfare. The argument is that risk and security can provoke strong emotions, which can be used to legitimise extraordinary measures, leading to practices that are otherwise indefensible (Davoudi, 2014).

While coming from fundamentally different original positions, both military urbanism and the safe city concept critically assess the role of security measures in smart cities and stress the need for a citizen-focus of new interventions. As such, they are relevant outlooks on security in the smart city and help to distinguish the special role security and crime prevention play in smart cities. In addition, both concepts tie in with the previously discussed criticism of traditional concepts such as SCP and the notion of positive criminology. They highlight the importance of considering both sides of the equation and emphasise the focus on citizens' needs and social fairness when deploying smart crime prevention and detection strategies (Von Hirsch et al., 2000).

2.4. Chapter Summary

This chapter has introduced the two themes that this thesis combines: surveillance and smart cities. Both theoretical and practical perspectives on surveillance and the smart city context were discussed, setting the stage for the empirical analyses presented in the following chapters. The theoretical underpinnings of this thesis, introduced in this chapter, will guide the analyses and will serve as underlying assumptions in the following discussions.

The chapter has further shown how surveillance and smart cities are inevitably linked. Smart cities depend on sensors and the large-scale gathering of data from all aspects of city life (Batty, 2013; Watzinger, 2019). This means that surveillance occurs more or less naturally as part of any smart city concept, even if it is not necessarily in the context of crime prevention or policing.

The significant changes to urban infrastructure that the smartification of cities promises offer a variety of both challenges and opportunities for surveillance and policing. Even though most smart city concepts mention security and safety as foundations of a liveable urban environment, many do not include specific plans for police surveillance for the purpose of crime prevention (this is further discussed in Chapter 3).

Chapter Three

Security Technologies and Their Functions in Smart Cities

3.1. Chapter Overview

The systematic review presented in this chapter explores the recent literature concerned with new 'smart city' security technologies and aims to investigate to what extent these new interventions correspond with traditional functions of security interventions. Based on an extensive systematic review of the literature this chapter compiles a list of security interventions for smart cities and suggests several changes to the conceptual status quo in the field. Ultimately, this chapter proposes three clear categories to categorise security interventions in smart cities: Those interventions that use new sensors but traditional actuators, those that seek to make old systems smart, and those that introduce entirely new functions. These themes are then discussed in detail and the importance of each group of interventions for the overall field of urban security and governance is assessed.

The results presented in this chapter have also been published in form of the following journal article:

- Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. Sustainable cities and society, 55, 102023. DOI: https://doi.org/10.1016/j.scs.2020.102023

3.2. Introduction

Rapid urbanisation and progress in information and communication technologies (ICT) are two of the most important phenomena impacting urban security planning and governance today (Cocchia, 2014; Zhu et al., 2019). The latter, especially, has shaped the concept of smart cities, an increasingly popular idea in recent years

(Albino et al., 2015; Naphade, Banavar, Harrison, Paraszczak, & Morris, 2011; Ralko & Kumar, 2016). Smart city technology is hailed as the solution to many urban challenges such as transportation, waste management, and environmental protection (Alawadhi et al., 2012; Ankitha et al., 2017; Gohar, Muzammal, & Rahman, 2018; Lella, Mandla, & Zhu, 2017; Zhang, Wan, Yang, & Yang, 2017a; Zhang et al., 2017b). While these issues are the focus of a growing debate about smart city development, aspects of security and crime prevention are often neglected (Ralko & Kumar, 2016).

As a result, the implications of new smart city security systems for crime reduction, security, and urban governance are rarely discussed. This systematic review attempts to address this gap by exploring the last ten years' worth of literature on new security technologies that can be considered to fall under the smart city concept. Overall, this chapter seeks to answer three core research questions, discussing how the academic literature conceptualises security technologies for crime prevention in smart cities, which specific technologies have been documented in the literature, and to what extent the functions of smart security technologies differ from traditional security technologies.

Through an extensive literature search and an analysis of 121 studies, this chapter compiles a list of security interventions for smart cities, discusses and contrasts their functions with those of more traditional interventions, before ultimately proposing several changes to the conceptual status quo in the field.

In the following, this chapter provides background information on the role of security in urban planning and smart cities. It then outlines the core methodological principles and search strategy used in this review before presenting and discussing the findings.

3.3. The Technical Components of the Smart City

Beyond the definitional issues addressed in Chapter 2 of this thesis, it is important to understand what a smart city practically entails and how it functions. It is difficult to conceive of a general architecture for smart cities because of the extremely diverse range of devices, technologies, and services that may be associated in such a system, and because of the high degree of interdependence between various components (Jalali, El-Khatib, & McGregor, 2015). As such, there are many different models that discuss what components and infrastructures a smart city needs (Gaur, Scotney, Parr, & McClean, 2015). Most, if not all, of these smart city architectures contain, however, three basic layers: A sensor layer, a network or processing layer, and a service or actuator layer (Filipponi et al., 2010; Gaur et al., 2015; Jalali et al., 2015; Zhang et al., 2017b). This distinction between the different layers is also useful to understand the smart city as a complex system made up of various components on different levels, reaching from single sensors to software and servers that integrate them and ensure communication between them (Zhang et al., 2017b). Crime prevention interventions in the sense of this thesis are thus specific technological solutions that seek to address a distinct (crime-related) problem and make up one or several components of a smart city infrastructure either on one or on multiple layers.

The sensor layer consists of the various (often heterogeneous) data collection units (i.e., sensors). These can be deployed to measure almost anything in the urban landscape (Lung, Sabou, & Buchman, 2015). Examples include environmental factors like brightness or sound, cameras, or RFID tags to monitor entire objects (Jalali et al., 2015).

Many smart cities rely, however, not only on permanently installed or fixed sensors but also include participatory sensing approaches that rely (sometimes exclusively) on human input. A good example of this are smartphones which have suddenly enabled billions of individuals to collect geo-tagged sensor measurements and media streams about their immediate spaces, such as an image or a sound clip or a temperature reading (Durga, Surya, & Daniel, 2018; Srivastava et al., 2012). Not only does this form of sensing naturally provide sensor coverage where relevant processes are happening, but it also uses the human expertise in operating the sensor to gather high-quality measurements (e.g., capturing high-quality images in a cluttered space with poor lighting or only recording relevant information as opposed to sensors that gather all data). This form of sensing may occur in a variety of ways, e.g., through the public posting of images online, the 'checking-in' at certain locations, or the use of certain data or Wi-Fi-networks.

As such, the sensor layer should not be seen as an exclusively technological component of the smart city but rather as one that also includes a human dimension. The diversity and heterogenous make-up of the sensing layer is crucial to capture a broad spectrum of data that can in subsequent steps be used to create a more complete picture of the situation (Oatley et al., 2015).

Data from this sensor layer is then delivered to the respective actuators via the network layer. This second layer provides the communication infrastructure to transport the data but also aggregates data from different sensors (Filipponi et al., 2010). The network layer also contains the capacity to process collected data and to translate it into readable (and actionable) information for the actuators (Filipponi et al., 2010; Jalali et al., 2015; Tian, Wang, Zhou, & Peng, 2018). This processing may take place in a centralised or decentralised fashion. In case of the latter, individual sensor units also possess processing power to manage recorded data (Al-Anbuky, 2014; Baldoni et al., 2017; Tian et al., 2018). Decentralised units or subsystems may have independent sensor-actuator loops but may also feed into the larger system of the smart city (Gil-Garcia et al., 2015; Jalali et al., 2015).

The last layer then contains actuators, i.e. those units that bring about a physical change in the environment or provide the required service (in this case fulfil a crime prevention or policing function) (Gaur et al., 2015). Such a function could be either purely technological, e.g., turning up street lights, raising an alarm, controlling traffic flows, or retractable barriers, they may also call for human involvement such as the deployment of a police patrol or security staff (Srivastava, Abdelzaher, & Szymanski, 2012).

The extensive literature search upon which these arguments are based sought to give an overview of the variety of functions new security technologies might fulfil. Overall, it aims to augment but also challenge the current conceptualisation of emergent technologies as crime prevention measures for smart cities. By switching the focus to the 'functions' of these technologies (i.e., their direct/proximal effects on the environment), this chapter seeks to bridge the gap between the bigger picture of safe cities and security on one hand and deeply technological solutions on the other. Most relevant for the ensuing discussion of smart security interventions are the sensor and the actuator layer, which is why they will be highlighted in the following.

Table 4: Examples of components on different layers of smart city infrastructure.

Sensor Layer[1]	**Network Layer**[1]	**Actuator Layer**[1]
RFID sensor	Transmission technologies	Retractable barricade
CCTV camera	Processing/computing units	Police response
Facial recognition camera	Compression/analysis software	Streetlights
Microphones	…	Speakers
Motion detection		Adaptable signage
WIFI-access points		UAV swarm
Crowd-sourcing app		Alarm
Light sensor		…
…		

[1] A single intervention may combine different components from one or multiple layers.

3.4. Literature Search

3.4.1. Search Terms

Two methods were followed to narrow down the search terms for this review. As the term ‘smart city’ is contested and not consistently used throughout the literature, this chapter used the results of Cocchia's (2014) study to supplement the search strategy. Cocchia found that there is no coherent definition of the word 'smart' and that its use (along with other related labels) is often arbitrary, while identifying several core terms that are frequently used interchangeably. In addition, scoping searches were carried out to find appropriate search terms related to security and crime prevention. Though using this first set of terms helped to narrow down the output of the search, it also meant that some potentially relevant studies that were not framed in terms of ‘smart cities’ may have been excluded. Nonetheless, for practical reasons, the decision was made to retain this explicit focus on smart cities.

Wildcards were used to include variants of words with the same word stem (e.g., ‘offend*’ would identify terms such as offend, offender and offending). The terms ‘police’ and ‘policing’ were preferred over the wildcard ‘polic*’ which returned an abundance of results related to policy. Thus, two categories of search terms were used:

1. Terms related to ‘smart city’, including ‘future city’, ‘intelligent city’, ‘digital city’

AND

2. Terms related to crime prevention, including ‘crim*’, ‘secur*’, ‘offend*’, ‘police’, ‘policing’, ‘law enforcement’

3.4.2. Inclusion/Exclusion Criteria

The results were screened against the following pre-set inclusion and exclusion criteria:

- Only literature from the past ten years was included (2009 - 2018) to ensure that interventions were most relevant to today's smart city environments.
- Only literature that was available in English and German was included for practical reasons.
- Literature that was otherwise unobtainable or that was missing full-text or abstract was also excluded.
- To circumvent the pitfall of publication selection bias, grey literature was included in the review (following Mlinarić, Horvat, & Šupak Smolčić, 2017; Wilson, 2009) as a review based on a biased collection of studies is likely to produce biased conclusions (Rohstein & Hopewell, 2009). However, this does not mean that all studies, regardless of quality, were included. Instead, grey literature was examined especially carefully as it does not undergo a peer review process and as such is more prone to bias (Adams et al., 2016).

After a first round of sifting with the above-mentioned criteria, the following hierarchically layered selection criteria were employed:

- Articles must have thematic relevance (e.g., articles that mentioned either of the search terms as part of an enumeration were not considered, e.g., '*smart city technology* encompasses advances in transport management, *crime prevention* and other city services).
- Outputs had to have a focus on technology (e.g., articles should introduce or evaluate new technologies). Because smart cities do to a large extent depend on the innovation of existing systems, works that suggested improvements to currently existing security interventions were also included.
- Outputs should be related to crime prevention or the improvement of public safety/security
- Outputs that focussed on new crime opportunities in smart cities rather than crime prevention were excluded. This included literature on

cybercrime opportunities or cybersecurity in smart cities unless they also made reference to opportunities to prevent those crimes.

3.4.3. Search Strategy for Identification of Studies

Searches were carried out on the following search engines:

- General databases: Scopus, Web of Science, Proquest, Zetoc
- Technology specific databases: IEEE Xplore, ACM Digital Library
- Grey Literature Databases: British Library EThOS; Open Grey did not return any results.

Backward and forward searches were carried out once relevant articles were identified. This, however, did not yield any additional results.

3.4.4. Filtering Stages

The reference list and sifting process were managed using the EPPI Reviewer 4 software. After all duplicates and articles that did not meet the basic inclusion and exclusion criteria were removed, the title and abstract of the remaining papers were scanned against the layered selection criteria. For those studies that were included based on title and abstract, the full text was reviewed against the same criteria again to ensure that only relevant studies would be included in the final analysis.

3.4.5. Inter-Rater Reliability (IRR)

To ensure good inter-rater reliability and to avert personal biases in the selection of the studies, the original coding results were verified by four other coders. Each of the coders was assigned a random sample of one hundred studies. The sample size was selected to ensure that coders became familiar with the criteria (Belur, Tompson, Thornton, & Simon, 2018). When the results were compared, there was a 94 per cent agreement between the four coders. In the case of most disagreements, the 'correct' coding (or that which was the final agreed coding) was usually that which had been agreed on by a majority of coders. Disagreements that remained were discussed in the group and brought to a resolution by elaborating the overall aim of the review. The discussions highlighted a lack of clarity on some aspects of the inclusion and exclusion criteria, especially on issues of research design, methodology, and type of outcome measure, but also more fundamentally about how to screen studies that did not meet the inclusion criteria but might nevertheless be relevant.

Following the suggestion by Feng (2014) to improve accuracy, chance agreement was removed from the estimation of reliability by calculating the κ-statistic (see also Belur et al., 2018; Viera & Garrett, 2005). With a κ-statistic of 0.81 and above in three of the four cases, near perfect agreement between the coders was achieved (Landis & Koch, 1977). Only in one case, a κ-statistic of 0.72 was reported, which however, still indicated substantial agreement (Landis & Koch, 1977). Overall, the inter-rater reliability tests indicated a high agreement between coders and thus strengthened the validity of this review.

3.5. Synthesis Approach

Though some authors such as Wilson (2009) suggest that the credibility of a systematic review depends more on the number of studies used than on the method of synthesis, the following paragraphs will still briefly introduce the approach taken for grouping and analysing the included studies.

While the aim of any synthesis is to generate new knowledge grounded in the information of the individual research studies, the right methodological path to this new knowledge is not set in stone and depends heavily on the individual review (Thomas, O'Mara-Eves, Harden, & Newman, 2017a). Since this review spans across a variety of academic disciplines and fields, a thematic synthesis approach was chosen as the modus of analysis as it is especially suitable for analysing multidisciplinary datasets (Thomas et al., 2017a).

To address the research aims, common themes across the included studies were identified and analysed in detail. As a starting point for this process, this review used conceptualisations of traditional security functions for both the sensor layer and the actuator layer (Borrion et al., 2014; Ekblom & Hirschfield, 2014) but then employed an iterative and flexible approach (Gough, Oliver, & Thomas, 2017). This means that while the review builds on a foundation of open questions and some secure initial concepts, it is equally thematically grounded in the studies it contains (Thomas et al., 2017a).

The initial concepts used in this review should be seen as a starting point that introduces a common language to compare and contrast the identified intervention, rather than a rigid theoretical framework. Their sole purpose was to provide a common denominator (i.e. the clustering of security technologies by their function) for developing new themes from the included studies (Boyatzis, 1998).

3.6. Initial Concepts

In the following, this chapter lay out key functions of security interventions both as sensors (i.e., for threat detection) and actuators (i.e., for crime prevention). The functions on both the sensor and the actuator layer are critical to the creation of effective and efficient security systems. Table 5 brings together two conceptualisations to form a new set of initial concepts. The table merges the functions contributing to threat detection as identified by Borrion et al. (2014) with the functions pertaining to crime prevention as identified by Ekblom & Hirschfield (Ekblom & Hirschfield, 2014). The network layer was left out because there are no distinct frameworks that specify different functions on this layer and because they are not uniquely pertaining to crime detection or prevention technologies.

Table 5: Security functions on different layers of smart city infrastructure.

Situation Awareness – Focus on Sensor Layer	**Intervention – Focus on Actuator Layer (after Ekblom & Hirschfield, 2014)**
Detect: e.g., determining the presence of certain anomalies, substances, individuals or behaviours (Hardmeier, Hofer, & Schwaninger, 2005)	**Defeat**: physically block access and movement or block/obscure the information that offenders want to collect
Authenticate: e.g., verifying that an individual is a member of staff or that they have the right to access (after Adey, 2002)	**Disable/Deny**: equipment helpful to offenders such as bugs or cameras
Identify: e.g., determining the name of a given chemical substance (Federici et al., 2005)	**Direct/Deflect**: offenders towards/away from place or behaviour
Locate: e.g., determining the location of individual passengers considered as potential threats to the infrastructure (Lee, Smeaton, O'Connor, & Murphy, 2005)	**Deter-known** offenders know what the risk of exposure is and judge it unacceptable so abandon/ abort attempt
Profile: e.g., classifying passengers who fit the profile of an offender for extra security checks (Sweet, 2008)	**Deter-unknown**: offenders uncertain what control methods they are up against, so again judge risk of exposure unacceptable
Track: e.g., following the movement of certain passengers through station premises (McCoy, Bullock, & Brennan, 2005)	**Discourage**: offenders perceive effort too great, reward too little, relative to risk, so abandon/abort attempt
	Demotivate: awakening, of offenders, emotions contrary to the mission, e.g., empathy with victims, removing excuses, coward image
	Deceive: offenders act on wrong information and are exposed to arrest or intelligence collection, frustrated, or mistakenly decide not to select this site as target
	Disconcert: causing offenders to make an overt involuntary movement or otherwise become startled

	Detect[7]: passive, and active exposure to make offenders self-expose by instrumental, expressive, or involuntary action; by making legitimate presence/ behaviour distinctive; and by improving capacity of people exercising security role to detect **Detain**: once offenders are detected, they must be caught and held (or credible identifying details obtained so they can be traced) **Inform** (i.e. communicate): e.g., raising an alarm or calling in armed units in response to a detected threat (Kirschenbaum, Mariani, Van Gulijk, Rapaport, & Lubasz, 2012) **Manage**: e.g., performing resource allocation, tasking and scheduling (Olive, Laube, & Hofer, 2009)[8]

3.7. Results

After the first rounds of sifting, 209 documents were included for full-text analysis (figure 1). Out of these, thirty-seven papers were not obtainable and a further fifty-one papers were excluded because their full text did not meet the predefined criteria. This left 121 studies to be included in the final synthesis based on full-text screening.

[7] Note that the function to detect on the actuator layer is distinct from that on the sensor layer. Actuators with the function to detect can – similarly to the detain function – be seen as an enforcement action with the goal of removing the offender presence, whereas sensors merely seek to detect anomalies or illicit action.

[8] While this function may in some cases be considered to refer to the network layer of an intervention, this review categorises it as an actuator. This is because managing the interplay of different interventions has a much more direct impact on security and crime prevention in a smart city context.

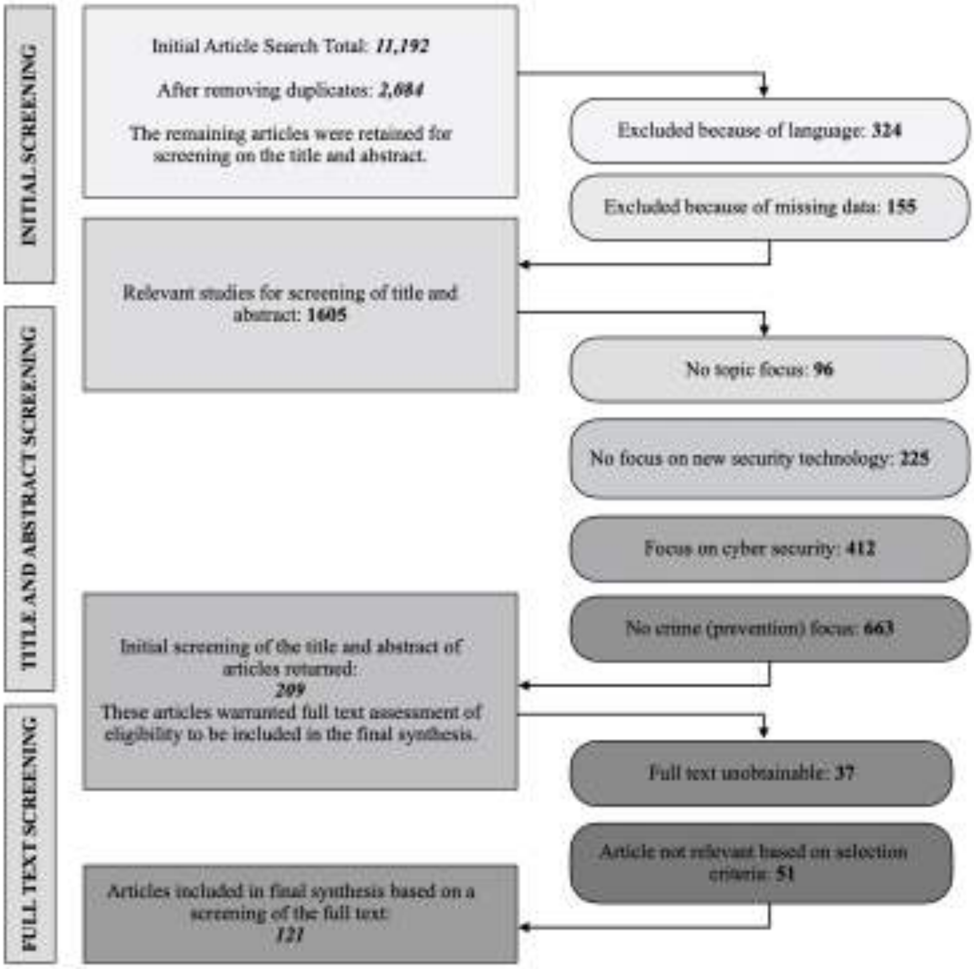

INITIAL SCREENING
TITLE AND ABSTRACT SCREENING
FULL TEXT SCREENING
Initial Article Search Total: 11,192
After removing duplicates: 2,084
The remaining articles were retained for screening on the title and abstract.
Excluded because of language: 324
Excluded because of missing data: 155
Relevant studies for screening of title and abstract: 1605
No topic focus: 96
No focus on new security technology: 225
Focus on cyber security: 412
No crime (prevention) focus: 663
Initial screening of the title and abstract of articles returned:
209
These articles warranted full text assessment of eligibility to be included in the final synthesis.
Full text unobtainable: 37
Article not relevant based on selection criteria: 51
Articles included in final synthesis based on a screening of the full text:
121

Figure 4: Search stages and results of the systematic review

Table 6: Results of the systematic literature search by category

New sensors, traditional actuators	**43**
Detect and prevent unwanted or criminal behaviour	34
Identify, authenticate, defeat (potential) offenders	9
Making old systems smart	**57**
Improve/automate processes in order to adjust them to a smart city environment	32
Manage/Integrate the interplay of different existing security solutions	25
Entirely new functions:	**21**
(Mass) information and crowdsourcing about criminal activity or public disorder	13
Predict potential threats	8

3.8. Analysis

Before detailing the content of the 121 included studies, it is worth making three general observations. Firstly, the search indicated that the literature on new crime prevention technologies and smart cities is characterised by a disparity between highly technical studies on one hand and conceptual studies on the other. While the former group of articles often neglects the bigger picture, the latter focusses on conceptual aspects of large smart city systems, usually with no real technological foundations. Only a few studies attempt to bridge this gap. Moreover, many works that seek to predict the future use of a specific technology become quickly outdated due to the fast-paced developments in the field.

Secondly, as smart cities are extraordinarily complex environments, there are many instances where single interventions fulfil multiple functions. This can either be multiple sensing or actuator functions or include a mix of both. The latter is especially the case for personal security systems such as the portable safety device proposed by Mahajan, Reddy, and Rajput (2018). The device comes in the form of a bracelet or small wearable item that automatically detects a threat to its wearer or can be manually triggered to a range of defensive mechanisms. While some of these functions were explicitly mentioned such as the raising of an alarm (inform), others were left implicit, such as deterrence effects or the triggering of other actuators that the technological solution may or may not have. Furthermore, the review identified a wide variety of technologies that do not explicitly carry out security or crime prevention functions by themselves, but which build upon and seek to improve existing technologies such as CCTV. With, fifty-seven included studies, this field makes up almost half of the identified interventions.

Thirdly, as already outlined in the background section of this chapter, there is no clear definition of smart cities or even of smart technologies. The definitional vagueness surrounding some of the core concepts of this nexus is clearly reflected in the literature, often leading to less meaningful conclusions and the lack of a common basis for discussion.

Despite these shortcomings of the overall field, three clear themes emerged from the technological interventions examined in this review. The first theme concerns new security technologies that fulfil clear traditional security functions such as to detect and prevent, or to identify, authenticate, and defeat (Section 3.8.1.). The second theme includes studies that are focussed on the process of improving and automating 'traditional' security functions (as outlined above), and those that contribute to the management and integration of services to create the bigger picture of a smart city (Section 3.8.2.). The last theme this review found is concerned with those interventions that fulfil new functions that as such did not really exist before, including disseminating mass information and predicting trends or events (Section 3.8.3.). Though many of these things may have been technically possible before, they lacked technological solutions that made a wide-scale deployment possible and feasible. In the following, these three themes will be described in more detail with regards to their aim, shortcomings, and implications for urban security, planning, and governance as a whole.

3.8.1. New Sensors, Traditional Actuators

3.8.1.1. Detect and Prevent

The search identified thirty-four interventions (Table 7) that aim to detect anomalies, threats, or unwanted behaviour. While some studies analysed human behaviour, facial expressions, or lip-movement to identify threats in individual people (Anagnostopoulos, 2014; Byun, Nasridinov, & Park, 2014; Rothkrantz, 2017b; Sajjad et al., 2018), others sought to detect fraudulent behaviour through the analysis of big data and crowd movement patterns (Cemgil, Kurutmaz, Cezayirli, Bingol, & Sener, 2017; Gupta, Chakraborty, & Mondal, 2017; Liu, Ni, & Krishnan, 2014; Rocher, Taha, Parra, & Lloret, 2018; Sadgali, Sael, & Benabbou, 2018). Even though many of these interventions operated to a large extent the sensor layer of the smart city and relied on already existent actuators, they often did include secondary functions. This included automatically informing the police if fraudulent or dangerous behaviour was detected (Venkatesan, Jawahar, Varsha, & Roshne, 2017), and actuators aimed at de-escalating situations through environmental modification such as changes in light, sound, or smell (Al-Anbuky, 2014; Schuilenburg & Peeters, 2018). Secondary functions were also included in the four interventions with the aim to track the movement of persons, vehicles, or UAVs, which in case a threat was detected, could independently contain it (Anees & Kumar, 2017; Brust et al., 2017; Reddy, Loke, Jani, & Dabre, 2018b; Saravanakumar et al., 2017) (Table 7).

Table 7: Interventions with the primary function to detect

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Cho (2012)	Visual emergency detection	Detection and recognition method for emergency and non-emergency speech.	detect	
Liu et al. (2014)	(Charging) fraud in Taxis	Uses GPS speed and location data to compute the actual service distance on the city map, and detect fraudulent behaviours	detect	
Byun et al. (2014)	Offender ID and prediction	Detect crimes in real-time by analysing the human emotions	detect	
Bourmpos, Argyris, and Syvridis (2014)	Prevention of crises (critical infrastructure)	Fibre sensing network to monitor diverse parameters of infrastructures, environmental conditions, and vehicle traffic	detect	
Giyenko and Im Cho (2016)	Faults of static CCTV	Intelligent IoT platform to facilitate the use of UAVs	detect	
Baba, Pescaru, Gui, and Jian (2016)	Stray dog attacks	Dangerous behaviour detection of group of stray dogs	detect	
Gupta et al. (2017)	Energy theft	Clustering based energy theft detection technique	detect	
Cemgil et al. (2017)	Fraud in meter readings	Fraud detection mechanism on the electricity consumption data	detect	
Welsh and Roy (2017)	Gunshot detection	Utilising ten different sensors to detect gunshots	detect	
Bellini, Cenni, Nesi, and Paoli (2017)	Monitoring the flow of people	System to monitor the use of WiFi access points to determine how and where traffic is flowing	detect	
Baldoni et al. (2017)	Faults of static CCTV	Capillary video surveillance platform using plug-and-play that is flexible and scalable with the number of transmitting and receiving devices	detect	
Cubik et al. (2017)	Perimeter protection	Use of fibreoptic sensors in perimeter protection.	detect	
Ertugrul, Kocaman, and Sahingoz (2018)	Mapping and surveillance of buildings	Autonomous UAVs for indoor mapping of buildings and physical security control	detect	

Table 7: Interventions with the primary function to detect (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Borges et al. (2017)	Detection of crime hot spots	Analyses characteristics of the urban environment to detect hotspots of criminal activities	detect	
Sajjad et al. (2018)	Facial expression recognition	Suspicious activity recognition based on facial expression analysis	detect	
Sadgali et al. (2018)	Credit card fraud	Detection of fraudulent transactions from big data using machine learning	detect	
Chackravarthy, Schmitt, and Yang (2018)	Backlog of video data created by traditional CCTV	Neural networks in combination with a Hybrid Deep Learning algorithm to analyse video stream data	detect	manage
Durga, Surya, and Daniel (2018)	Faults of static CCTV	Android application that obtains video feed, images and sound clips from the users and then uses cloud services for video enhancement and restoration of the content	detect	
Calavia, Baladrón, Aguiar, Carro, and Sánchez-Esguevillas (2012)	Faults of static CCTV	Intelligent video surveillance system able to detect and identify abnormal and alarming situations by analysing object movement	detect	authenticate
Datta and Sarkar (2017)	Faults of static CCTV	Flexible surveillance system using smart phones, existing sensors, as well as home automation	detect	authenticate
Hu and Ni (2018)	Vehicle/object detection + license plate recognition	Automated object detection for urban surveillance systems	detect	authenticate
Manasa (2016)	Concealed explosives	Nanoscale technologies to find hidden explosives.	detect	identify
Agha, Ranjan, and Gan (2017)	Illegal racing/tail pipe modification	Automatic noisy vehicle surveillance camera	detect	identify
Rocher et al. (2018)	Fraudulent use of dyed fuels	IoT system to detect the presence of low-taxed fuels in the deposit of cars	detect	identify
Rothkrantz (2017a)	Sound recognition in CCTV	Lip-movements of a talking mouth can be recorded and understood, and aggressive behaviour detected	detect	improve

Table 7: Interventions with the primary function to detect (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Venkatesan et al. (2017)	Theft	IoT based security system for homes, offices, banks. Sensors for theft and fire detection. Can automatically notify the user and automatically captures images of the intruder.	detect	inform
Ahir, Kapadia, Chauhan, and Sanghavi (2018)	Harassment, molestation	Smart device for women, including GPS/vital tracking, alarm, force sensor, and shock function	detect	inform
Eigenraam and Rothkrantz (2016)	Traffic rule violations/ suspicious behaviour	Multi-camera surveillance systems designed as a Decision Support System (DSS)	detect	locate
García, Meana-Llorián, G-Bustelo, Lovelle, and Garcia-Fernandez (2017)	Faults of static CCTV	Analysis of pictures through Computer Vision to detect people in the analysed pictures	detect	manage
Anagnostopoulos (2014)	Suicide in metro stations	Information system architecture which can predict whether an individual intends to commit a suicide	detect	predict
Al-Anbuky (2014)	Street crime	Sensor-actuator smart public lighting network	detect	prevent
Schuilenburg and Peeters (2018)	Crime in night-time economy	Sound, smell, and lighting programming combined with data analysis is used to reduce violence and aggression	detect	prevent
de Diego, San Román, Montero, Conde, and Cabello (2018)	Faults of static CCTV	Distributed intelligent video surveillance architecture based on Wireless Multimedia Sensor Networks	detect	track
Huang and Chu (2017)	Trapped people	Detect trapped victims underneath fallen objects	detect	Track

Table 8: Interventions with the primary function to track and containment function

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Saravanakumar et al. (2017)	Vehicle theft, speeding	Track vehicles that commit crime and enable decision making at neighbouring traffic sites.	track	contain
Brust et al. (2017)	Malicious UAVs	UAV defence system for the purpose of intercepting and escorting a malicious UAV outside the flight zone.	track	contain
Reddy et al. (2018)	Re-identification in CCTV	Facial recognition system to track or search a target person from a real time video feed	track	improve
Anees and Kumar (2017)	Crowd-density scanning	Key-point descriptors extracted from the scene are used to compute the dense areas which is further used to define the direction of the flow	track	manage

Technologies for the detection of threats through the collection and use of large amounts of data and technological measures to prevent crime long existed and are in widespread use today (e.g., CCTV). The automatic and local containment of unwanted behaviour or dangerous situations without the involvement of the broader security infrastructure (e.g., police services) or in some cases any human input is, however, new. Interventions that fall into this category often bring sensor and actuator layer closer together by creating a single intervention or by changing or adding new actuators to the equation. This does not only have an impact on crime prevention but also on urban planning and governance processes as a whole. Self-contained interventions pose fundamentally different requirements to urban planning and governance than those that require external actuators such as police interventions. An example of this are audio sensors that, if commotion is recognised, turn up the streetlights rather than triggering more traditional actuators like a police response (Al-Anbuky, 2014; de Kort et al., 2014). Because these interventions rely on the interplay of different smart city components to alert authorities, self-contained security interventions rely on the broad deployment of smart infrastructure across other realms such as lighting and the far-reaching deployment of more elaborate sensors and actuators (de Kort et al., 2014). This is also emblematic of the difficulties inherent in the retrofitting of existing cities with smart technologies brings about. Because smart interventions rely so heavily on each other and because a broad deployment across various realms opens up a variety of possibilities, it is inefficient to 'divide and conquer', i.e. to modernise sector after sector (Rathore et al., 2016; Zygiaris, 2013). Since the usefulness of self-contained interventions is highly dependent on a holistic approach, it poses significant challenges to current processes of urban governance and especially modernisation efforts. Thus, interventions that are made up of not only sensor technology but also of actuators that automatically contain a threat can potentially have a great effect on urban security as a whole.

In addition to these more practical requirements, crowdsensing and big data analytics promise some degree of privacy for individuals, whereas facial or motion recognition technologies rely on singling out persons from the larger group (Balla & Jadhao, 2018; Braun, Fung, Iqbal, & Shah, 2018). As such, the studies examined show that interventions that rely on motion or facial expression recognition are especially controversial in terms of privacy, bringing many new ethical considerations and requirements into the planning process for urban security (Marx, 1998; Parra & Lopez, 2017). These considerations are not only important to ensure an inclusive and rigorous data-protection regime in smart surveillance environments, but they also have operational significance for the planning, deployment, and often functioning of these security measures (Patton, 2000).

3.8.1.2. Identify, Authenticate, Defeat

These initial findings tie in with the five included studies (Table 9) that aimed to authenticate individuals or vehicles attempting to access a restricted area (be it a private property or a congestion zone in a city). Operationally, this was done either through Near Field Communication (NFC) (Castella-Roca, Mut-Puigserver, Payeras-Capella, Viejo, & Angles-Tafalla, 2017) or through camera surveillance systems relying on automated license plate recognition (Balla & Jadhao, 2018; Boukerche, Siddiqui, & Mammeri, 2017; Hadjkacem, Ayedi, Abid, & Snoussi, 2017; Rothkrantz, 2017a). While the latter to some extent often constituted an improvement or automation of an existing system, the interventions were considered distinct because they are independent systems for access control that could also be implemented without any prior interventions in place. As such, the systems posed a significantly lesser challenge to urban security planning than those mentioned in the previous section.

Table 9: Interventions with the primary function to authenticate

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Castella-Roca et al. (2017)	Vehicle access to restricted zones	Driver's smartphone is used to validate the access to a restricted zone	authenticate	
Balla and Jadhao (2018)	Unauthorised access	Intelligent security system using facial recognition	authenticate	
Sajjad et al. (2017)	Identification of suspects	Cloud assisted facial recognition framework	authenticate	identify
Rothkrantz (2017b)	CCTV does not operate in real time	Use of surveillance cameras to localise and recognise faces from suspect individuals	authenticate	improve
Boukerche et al. (2017)	Vehicle re-identification	Automated vehicle detection and classification system.	authenticate	profile

The effectiveness of these measures relies to a large extent on the use of physical barriers to 'defeat' intruders or the threat of repercussions if they are caught violating access rules (e.g., fines). Access control measures have, however, especially in a smart city far more use than the explicitly mentioned actuators might suggest. Holistic smart city architectures could for example not only prevent vehicles from entering a controlled zone but could also track movement patterns and impose automatic fines (Barba, Mateos, Soto, Mezher, & Igartua, 2012). This would alleviate the need for controlling access to congestion or environmental protection zones in city centres by the police and thus save resources in the long run. The deployment of such smart access control measures could additionally help the expansion of 'greener' transportation and as such would positively impact other realms of smart city development in the future (Barba et al., 2012).

In addition to these static access control measures, Sajjad et al. (2017) introduce a cloud-assisted face recognition framework. They propose the use of nano-devices for a concealed and secure face recognition system. Wearing a small-sized portable wireless camera and a small processing unit for face detection and recognition on officer's uniforms would allow for the identification of anyone police interact with, without the need for manual identification. While this is only an example, it is symbolic for a move to supplement current static CCTV systems through mobile components. Whether this includes body worn cameras, cars, or drones, it has the potential to severely change the way we think about urban surveillance. This has some clear benefits such as the ability for cameras to follow crime and to surpass issues of re-identification between cameras if suspects are on the move (Zhang & Yu, 2018).

Nevertheless, these benefits come at a cost. While most of the systems proposed in the literature are often minimally intrusive and offer maximum amounts of privacy (Castella-Roca et al., 2017), the use of wearable facial recognition devices, as proposed by Sajjad et al. (2017) should be seen as problematic. Though the system may offer some use to the police, the potential downsides of its deployment are grave. It would for example mean that police officers could not be approached without citizens being subject to facial recognition, which in turn may dissuade many from approaching the police. This has important implications for citizens in their relations and contacts with police actors. This intervention in particular shows that privacy and data protection concerns are not only important on a legal level but also raise the question to what extent an intervention like this can have negative consequences for existing measures and in how far it can be reconciled with the citizen focus of the smart city concept (Braun et al., 2018).

3.8.1.3. Section Summary

Overall, this study has identified a substantial body of literature concerned with using new sensors to detect criminal behaviour and identify individual perpetrators, often relying on already existing actuators for deterrence and crime prevention. Many of the identified interventions could transform urban security and the vision of a safe city. They reinforce the idea that in a smart city, many new security interventions rely on the broad deployment of smart technologies across different realms of the urban environment. Because security interventions no longer only rely on input from the police or their own sensors but can draw from a broad array of data sources, they become significantly more all-encompassing and holistic. Security measures no longer rely solely on the policy or a far-reaching security apparatus in a city but their effectiveness also relies on smart technologies in other realms such as street lighting or traffic management (Vitalij, Robnik, & Alexey, 2012). A lack of smartification in one realm can thus have impacts on the effectiveness of interventions in all other realms, first and foremost security interventions. This has great implications for the planning process of smart cities and their security infrastructure itself and shows that future security infrastructures are not separate systems but both reliant on and a prerequisite for the deployment of smart systems across other realms of city services.

This, however, does not mean that new interventions are uncontroversial. Privacy and data protection issues are at the forefront of concerns that may arise with their deployment and that need to be addressed in the planning and deployment of safe city concepts (Braun et al., 2018). As such, the interventions clustered in this theme offer great potential, but also require a thorough and far-reaching rethinking of the planning process itself because systems become significantly more interconnected and the effectiveness of single components dependent on the broader infrastructure (Mishra & Kumar, 2013).

3.8.2. Making Old Systems Smart

3.8.2.1. Improve/Automate

While many of the previously introduced measures sought to introduce entirely new systems, this is often neither necessary nor feasible. Instead, old systems that function well and are already in place can be improved and processes automated in order to adjust them to a smart city environment. This review identified thirty-two studies that address this issue (Table 10).

Table 10: Interventions with the primary function to improve or automate

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Sadha (2015)	Faults of static CCTV	Parallel architecture for smart video surveillance	improve	
Sormani et al. (2016)	No datasets for training algorithms	Generation of datasets for training reasoning algorithms for predicting the likelihood of terrorist actions against specific assets and locations in urban environment	improve	
Xiong et al. (2017)	Re-identification in CCTV	Multiple deep metric learning method empowered by the functionality of person similarity probability measurement	improve	
Shi, Ming, Fan, and Tian (2017)	Facial recognition	Recognition algorithm based on multi- scale completed local binary pattern	improve	
Zheng et al. (2015)	Re-identification in CCTV	Weight-based sparse coding approach for person re-identification	improve	
Salmerón-García et al. (2017)	Faults of static CCTV	Cloud-based surveillance system.	improve	
Thomas et al. (2017b)	Faults of static CCTV	Video summarisation to reduce amounts of data recorded	improve	
Singh, Patil, and Omkar (2018)	Computational cost in multiple object tracking.	Parallel solution which effectively handles the challenges of time-dependencies among the various sections of the video file processed during multiple object tracking	improve	
Saba (2017)	Latency issues in CCTV	Device to capture and compress images and mounted with PIR sensor to detect movement	improve	
Tian et al. (2018)	Faults of static CCTV	Block-level background modelling (BBM) algorithm to support long-term reference structure for efficient surveillance video coding	improve	
Hadjkacem et al. (2017)	Re-identification in CCTV	New approach based-on the analysis of all the video data extracted from camera-networks	improve	manage

Table 10: Interventions with the primary function to improve or automate (continued)

Author (Year)	**(Crime) Problem**	**Solution**	**Primary function**	**Secondary function**
Zhang et al. (2015)	Re-identification in CCTV	Real-time distributed wire-less surveillance system that leverages edge computing to support real-time tracking and surveillance	improve	manage
Tan and Chen (2014)	Faults of static CCTV	Approach for fast and parallel video processing	improve	manage
Zhou et al. (2015)	Faults of static CCTV	Using existing public bus transit system to collect data from the cameras and physically transport it to the bus terminus, to be uploaded to the data centre	improve	manage
Oza and Gohil (2016)	Faults of static CCTV	Cloud based surveillance system for live video streaming	improve	manage
Xu, Mei, Liu, Hu, and Chen (2016)	Faults of static CCTV	Semantic based cloud environment to analyse and search surveillance video data	improve	manage
Valentín et al. (2017)	Faults of static CCTV	Architecture for automated video surveillance based on cloud computing	improve	manage
Wang, Pan, and Esposito (2017)	Faults of static CCTV	IoT based elastic surveillance system using edge computing to perform data processing	improve	manage
Zhang et al. (2017a)	Human action recognition	Background modelling method from surveillance video	improve	manage
Mehboob et al. (2017)	Faults of static CCTV	3D conversion from traffic video content to Google Maps	improve	manage
Zingoni, Diani, and Corsini (2017)	Moving object recognition	Algorithm capable of successfully recognising and classifying moving objects	improve	manage
García, Valentín, Serrano, Palacios-Alonso, and Sucar (2017)	Faults of static CCTV	Visualisation techniques for both local and global visualisation	improve	manage
Ramírez, Barragán, García-Torales, and Larios (2016)	Transmission latency of data (CCTV)	Wireless sensor network (WSN) using low-power devices for the transceiver process to improve the data management using both, storage, and transmission data	improve	manage

Table 10: Interventions with the primary function to improve or automate (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Ma et al. (2018)	CCTV placement	Use of traffic patterns to improve the placement of CCTV cameras	improve	manage
Pereira et al. (2018)	Faults of static CCTV	Low-cost smart surveillance platform designed to create a ubiquitous environment	improve	manage
Memos et al. (2018)	Faults of static CCTV	Algorithm to use less memory at the wireless sensor nodes	improve	manage
Peixoto et al. (2018)	Faults of static CCTV	Gap filling algorithms to data missing problem in a smart surveillance environment	improve	manage
Kumar, Datta, Singh, and Sangaiah (2018)	Faults of static CCTV	Intelligent decision computing-based paradigm for crowd monitoring	improve	manage
Miraftabzadeh, Rad, Choo, and Jamshidi (2018)	Re-identification in CCTV	Algorithm to extract and administrate the crowd-sourced facial image features (e.g., social media platforms and multiple cameras in a dense crowd, such as a stadium or airport)	improve	manage
Zhang and Yu (2018)	Re-identification in CCTV	Deformable convolution module to the traditional baseline to enhance the transformation modelling capability without additional supervision	improve	manage
Al-Shami, Zekri, El-Zaart, and Zantout (2017)	Traffic rule violations	Parallelization processes that enable the online processing of images by an embedded system	improve	manage
Jun et al. (2017)	Faults of static CCTV	Collaboration-based Local Search Algorithm (COLSA)	improve	manage

The key premise of these studies is that current surveillance systems need improvements to be useful in the future. The scalability and cost-effectiveness of current systems depends largely on these improvements as increased amounts of data and the need for faster processing, drive demand for innovation (Valentín et al., 2017). The most prominent example of this are many video surveillance platforms in use today, which are presented with severe problems of efficiency and scalability when the numbers of data flow senders and receivers increase (Baldoni et al., 2017).

In addition, the scalability of modern surveillance systems is often limited by the human factor in a variety of ways, driving the demand for automation (e.g., human operators can watch ten cameras, but will not be able to monitor 10 000 deployed sensors).[9] Many studies that sought to automate processes that currently require manual input, focus on human re-identification in multi-camera surveillance networks (Hadjkacem et al., 2017; Zhang et al., 2017b; Zheng, Sheng, Zhang, Zhang, & Xiong, 2015) or even introduce a wholistic automated system architecture that do entirely without human operators (Valentín et al., 2017). The latter, in particular, is needed to realise the complex system that is a smart city because it does not tackle the issue on merely one layer but improves sensors, processing, and actuators alike. These developments are also problematic when examining current planning processes for security infrastructure. In many instances, there is a disparity between private developments and security agencies. And even where security and crime prevention are considered as factors, developments are often planned with already or soon-to-be outdated systems (Morton, Horne, Dalton, & Thompson, 2012; Sandborn, 2007).

[9] While human-technology interaction is clearly more complex than this, the chapter emphasises the point that many systems are limited in functionality and scalability by the human factor rather than technological elements. This is not to circumvent valuable debates on the social environments needed for such technologies but rather to highlight the functional limitations introduced by human involvement.

Due to steadily improving camera and sensor technology and their large-scale deployment, data streams are exploding in urban surveillance. This impacts the scalability of current systems massively as they 'outgrow' the current infrastructure (Brayne, 2017). These issues of scalability of older systems are tackled by interventions on the processing layer of the smart city, aimed at making the transmission, storage, and processing of data cheaper, easier, and faster (Memos, Psannis, Ishibashi, Kim, & Gupta, 2018; Saba, 2017; Singh, Majumdar, & Rajan, 2017; Thomas, Gupta, & Subramanian, 2017b; Zhou, Saha, & Rangarajan, 2015). While in this case, the processing layer plays a significant role as the key variable limiting the growth and the flexibility of the systems, it is also sensors and actuators where innovation has a relevant impact on crime prevention in the future.

Future systems aim to analyse data in real-time using AI to allow for a quicker response in case of danger (Reddy et al., 2018b; Zhang, Chowdhery, Bahl, Jamieson, & Banerjee, 2015). Because in many cases not enough historical data exists to train AI, or because the data has gaps that could affect the machine learning, some studies introduce approaches to generate dummy data that can be used for training (Peixoto et al., 2018; Sormani et al., 2016). Such approaches are especially noteworthy because they do not only address shortcomings of current crime prevention technologies but rather provide practical solutions to aid the deployment of other interventions.

Similarly, studies such as those of Ma et al. (2018) and Jun, Chang, Jeong, and Lee (2017) highlight the need for improving not only existing software and hardware but also the methods and procedures by which the deployment of technologies is determined. Ma et al. (2018) discuss new metrics for the sensible deployment of surveillance cameras but the essence of their research is transferable to many other contexts; if the urban landscape changes significantly, parameters for the allocation of security technologies will also change. Unless this is considered along the way, the planning of urban security runs danger of missing crucial developments and ultimately failing in the future.

In terms of urban security as a whole and implications for its planning, interventions that seek to improve and automate current security measures fulfil one of the most important functions. This is because in practice, only in few cases smart cities are built from the ground up. Thus, when speaking about building smart cities, we often mean the retrofitting and improvement of existing systems with smart technologies (Habibzadeh, Soyata, Kantarci, Boukerche, & Kaptan, 2018). As such it is crucial that we approach the smartification of cities holistically while maintaining an eye for existing infrastructures as the basis for these developments.

3.8.2.2. Manage/Integrate

A truly safe (smart) city is defined by increased integration of different systems and the boundary-less coordination of measures across all fields. This review identified twenty-five interventions that sought to integrate or to manage the interplay of different existing security solutions in urban environments (Table 11). The scope and focus of these interventions differed greatly, reaching from single-layer solutions tackling the complex interplay of different sensors (Camboim, Neto, Rodrigues, & Zhao, 2017; Chen, Xu, & Guo, 2013) to holistic integrated framework architectures that work to connect sensors and actuators across the city (Bartoli, Fantacci, Gei, Marabissi, & Micciullo, 2015; Dbouk, Mcheick, & Sbeity, 2014; Fernández et al., 2013; Khan, Azmi, Ansari, & Dhalvelkar, 2018; Liu et al., 2017b; Vitalij et al., 2012). The aim of the interventions is in many cases the more efficient use of resources (Al-Muaythir & Hossain, 2016; Hochstetler, Hochstetler, & Fu, 2016) but also the improvement of services through management and integration of different measures (Kunst, Avila, Pignaton, Bampi, & Rochol, 2018).

Table 11: Interventions with the primary function to manage or integrate

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Khan et al. (2018)	Large quantities of call data records	Use of the call data records (CDRs) of various suspects and victims in order to extract significant evidence	manage	investigate
Dbouk et al. (2014)	Terrorist attacks	Surveillance system architecture	manage	
Bartoli et al. (2015)	Growing populations and demand to respond	Integrated platform for new generation professional mobile radio system, wireless sensor networks, social networks, and a data gathering and analysis system able to collect and elaborate heterogeneous information coming from different sources	manage	
Al-Muaythir and Hossain (2016)	Limited resources/inflexible systems	Parametric subscriptions/cloud-based publish/subscribe framework	manage	
Hochstetler et al. (2016)	Limited resources	Network of clusters to efficiently assign patrols based on informational entropy in order to minimise police time-to-arrival and the overall numbers of police on patrol	manage	
Lohokare, Dani, Sontakke, Apte, and Sahni (2017)	Response time	Capturing live location of the emergency services to connect them directly to nearest citizen in need	manage	
Duan, Lou, Wang, Gao, and Rui (2018)	Faults of static CCTV	AI oriented large-scale video management. Person/vehicle re-identification, facial recognition before coding	manage	
Hartama et al. (2017)	Emergency traffic management	Strategy related to efforts to improve the distribution of space and time based on traffic volume	manage	

Table 11: Interventions with the primary function to manage or integrate (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Hosseini, Salehi, and Gottumukkala (2017)	Oversubscription of servers with relevant video feeds	Stream-priority aware resource allocation mechanism to enable interactive video prioritisation without a major impact on the flow of non-prioritised video streams	manage	
Patel, Wala, Shaba, and Lopes (2018)	Inefficient police records	Proposed online system for police stations to help digitalise their work	manage	
Dey, Chakraborty, Naskar, and Misra (2012)	Faults of static CCTV	Multimedia surveillance backend system architecture based on the Sensor Web Enablement framework and cloud-based 'key-value' stores	manage	improve
Chen et al. (2013)	Faults of static CCTV	New architectures integrated with Hadoop to resolve the urgent pressure of overloaded and to put the whole system into the computer cluster	manage	improve
Khorov, Gushchin, and Safonov (2015)	Faults of static CCTV	Easy implementation strategy to drop the smallest (in bytes) video frame whenever queue overflows	manage	improve
Lei et al. (2016)	Large quantities of data	K-means algorithm that can automatically split and merge clusters which incorporates the new ideas in dealing with huge scale of video data	manage	improve
Chen et al. (2016)	Faults of static CCTV	Dynamic video stream processing scheme to meet the requirements of real-time information processing and decision making	manage	improve
Pribadi, Kurniawan, Hariadi, and Nugroho (2017)	CCTV placement	Algorithm for improved camera placement.	manage	improve
Rametta, Baldoni, Lombardo, Micalizzi, and Vassallo (2017)	Faults of static CCTV	Smart CCTV platform to exploit the facilities offered by full SDN-NFV networks.	manage	improve

Table 11: Interventions with the primary function to manage or integrate (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Liu and Lin (2017)	Automated license plate recognition	Hierarchical architecture combining supervised K-means and support vector machine.	manage	improve
Wu et al. (2017)	Data management in GIS	Hybrid database organization and management approach with SQL relational databases (RDB) and not only SQL (NoSQL) databases	manage	improve
Kunst et al. (2018)	High amounts of data traffic lessen the quality of service.	Multi-purpose real time video surveillance application using resource sharing	manage	improve
Duan et al. (2018)	Faults of static CCTV	Computational methodology for reorienting, repositioning, and merging camera positions within a region under surveillance	manage	improve
Camboim et al. (2017)	Vehicle theft, violent crime	Smart surveillance system to recognise security threats in real time	manage	improve
Vitalij et al. (2012)	Lack of integration between different parts of smart cities.	Integrated framework with intelligent video surveillance, emergency communication, general alarm/local notification systems, environmental monitoring and forecasting, local fire/chemical control systems, spotting, position location / eCall, ERA- GLONASS services, communications, and mass media	manage	improve
Liu et al. (2017b)	Integration of different data sources	Community safety oriented public information platform	manage	integrate
Fernández et al. (2013)	Vandalism prevention, perimeter security	Intelligent surveillance platform based on the use of large numbers of cheap sensors	manage	detect

While it may at first seem as if the interventions collected in this category are not as relevant to security because they do not directly introduce new sensors or actuators (i.e., do not execute crime prevention tasks as such), they, in fact, take a central role in the security aspect of safe cities. This is especially relevant for safety and crime prevention planning and urban governance because larger quantities of information are transported and processed faster than before. This means not only that policies and decisions can rely on a more larger evidence base but also that decision making processes may need to change.

The integration of different security measures and their improved management through the deployment of connected systems is a prerequisite for the smart city (Ralko & Kumar, 2016). And because urban trends are heading in this direction, it is imperative that planners embrace the opportunities that come with it in all administrative procedures and planning processes to maintain the ability to solve urban problems in the future.

3.8.2.3. Section Summary

Overall, many of the interventions clustered in this theme aim to enable smart city developments through the increased improvement and integration of city service infrastructure and its technological components. Despite this clear aim, the approaches taken in the literature differ substantially. While some studies approach smart city efforts on a micro-level (i.e., single layer), others propose holistic systems for the management of different services from sensors and processing units to actuators. This variety of approaches highlights the fact that smart city security infrastructure depends on integration on all levels, between and within the different parts of the surveillance and security apparatus (Hall et al., 2000).

This category of interventions is also crucial because it is most likely to be realised in practice. Only rarely are smart cities built from the ground up, and a more realistic path is the gradual improvement of existing systems (Mishra & Kumar, 2013). In this context, it is important to remember that smart security measures and the concept of the safe city are not born from the overwhelming failure of existing interventions but rather from the wish to improve existing efforts and to make them more efficient and manageable in the future (Truntsevsky et al., 2018). As such, the interventions mentioned in this theme are not only practically appropriate, but they are also closest to the reality of financial and resource constraints in cities today. Given this it is surprising that only few studies (Al-Muaythir & Hossain, 2016; Hochstetler et al., 2016; Jun et al., 2017; Pereira et al., 2018) consider the economic implications or the financial efficiency of their interventions as a relevant factor in their deployment and evaluation. Despite the fact that efficiency and effectiveness are crucial factors in a smart city environment, this chapter found many studies discussing operational efficiency in terms that were far from today's urban realities.

3.8.3. Entirely New Functions

3.8.3.1. (Mass) Information and Crowdsourcing

While the original framework suggested an 'inform'-function limited to sounding alarm or alerting security services, this chapter suggests that this definition should be revised. In total, this chapter reviewed 13 studies that aimed to inform (i.e., communicate information about a specific situation) (Table 12). Only three of the interventions, however, functioned to automatically trigger actuators like alarming security services of a crime (Liu, Warade, Pai, & Gupta, 2017a; Mahajan et al., 2018; Nasui, Cernian, & Sgarciu, 2014). The other interventions were either user focussed on providing information about crime and crime prevention to the population (Ballesteros, Rahman, Carbunar, & Rishe, 2012; Kagawa, Saiki, & Nakamura, 2017; Mata et al., 2016; Peng, Xiao, Yao, Guan, & Yang, 2017; Truntsevsky et al., 2018) or fulfilled a hybrid role. To distinguish these two different groups, this chapter will refer to the latter as 'mass information', while the former will be labelled as interventions with the aim to 'inform'. All of the studies are listed in Table 12 below.

Table 12: Interventions with the primary function to crowdsource or provide information

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Ballesteros et al. (2012)	Lack of awareness in dangerous situations	Combined use of personal mobile devices and social networks to make users aware of the safety of their surroundings.	(mass) inform	
Mata et al. (2016)	Mobile applications do not show safe routes	Approach to provide estimations defined by crime rates for generating safe routes in mobile devices.	(mass) inform	
Peng et al. (2017)	Inaccurate information	Urban safety analysis system to infer safety index from multiple cross-domain urban data	(mass) inform	
Kagawa et al. (2017)	Lack of information	PRISM (Personalized Real-time Information with Security Map)	(mass) inform	
Truntsevsky et al. (2018)	Street crime	Exploring the possible application of modern digital technologies in the evaluation and prevention of crime.	(mass) inform	
Arauz et al. (2017)	Corruption	Platform to integrate user orientation, application of standards for the development of the city and citizen participation.	inform	
Carreño et al. (2015)	Personal security	A mobile application which implements participatory sensing to help people be aware of the risks that appear to exist in a certain place at a certain time.	(mass) inform	
Moreira et al. (2017)	Inefficient information for citizens	Mobile application as an alternative communication channel between public safety agencies and population.	inform	
Ferreira et al. (2017)	Assaults and street crime	Smart surveillance cameras system, a back-office system with a workflow engine and a mobile application within a collaborative concept	inform	

Table 12: Interventions with the primary function to crowdsource or provide information (continued)

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Bonatsos, Middleton, Melas, and Sabeur (2013)	Fear of crime/lack of awareness/misconceptions	Decision-support system integrating information, data and software modules representing city assets, hazards and processing models that simulate exposures to risks and potential compromise to safety and security.	inform	
Mahajan et al. (2018)	Assault, violence, attacks against women	Wearable/portable system that creates a sense of safety among women with a range of different features (automatic alarm, shock, audio streaming, location)	inform	
Nasui et al. (2014)	Transportation safety	Cloud based student transportation safety system is a location aware mobile asset management solution for operators of commercial fleets, having a cloud-based platform at its core.	inform	detect
Liu et al. (2017a)	Street crime	Fine-grained location-aware smart campus security systems that leverages hybrid localisation approaches with minimum deployment cost.	inform	detect

Despite their different foci, both types of intervention increasingly involve the use of mobile applications to crowdsource information about criminal activity or public disorder. While some of these applications create a knowledge base that in turn aims to inform users (Carreño, Gutierrez, Ochoa, & Fortino, 2015; Ferreira, Visintin, Okamoto, & Pu, 2017; Moreira, Cacho, Lopes, & Cavalcante, 2017), other applications, such as the online platform developed by Arauz, Moreno, Nancalres, Pérez, and Larios (2017), seek to tackle specific problems such as corruption by allowing users to report criminal activity directly to the authorities.

When assessing the effect these interventions have on the larger picture of urban security, it is important to distinguish between their different functions. While on one hand, mobile applications may be useful for mass information, i.e., to reach a large part of the population and to create broad awareness about crime and crime prevention, they also have downsides.

The most obvious issue of mobile applications is that their functionality and their ability to crowdsource information relies heavily on an active user base — without a crowd, no crowdsourcing. Even (or especially) if they are actively used, however, user-centric applications are open to misuse (Yang, Zhang, Ren, & Shen, 2015). Malicious actors may report false crimes to purposefully waste police resources or to put someone else in the crosshairs of security services. Another concern is that criminals could use apps just like the genuine user but to determine where victims might move to in order to avoid crime (Monahan & Mokos, 2013).

As discussed above, smart security technologies are aimed at making public services more efficient and effective and ultimately freeing up resources. This, however, is a double-edged sword, as 'inform'-functions make especially clear. While crowdsourcing information about crime with the goal of increased reporting of a certain type of crime can be considered an innovation on the sensor layer and may be desirable, it may in other cases put an unnecessary strain on already tight resources and overwhelm existing actuators. For example, an increased report rate for domestic abuse may very well save lives, but an app that floods police with hundreds of reports of anti-social behaviour or noise complaints may in the end take up disproportional amounts of resources (Elliott-Davies, Donnelly, Boag-Munroe, & Van Mechelen, 2016). While interventions might be able to create a large network of 'eyes on the street' (Cozens & Davies, 2013; Hillier & Cozens, 2012), they may also create a flood of information that could overwhelm many public institutions.

Nonetheless, these interventions do offer some potential benefits. Especially crowd sourcing and mass information platforms can bring citizens and governments closer together (Kim & Lee, 2012). Apart from streamlining city services, e-participation can allow citizens to interact more directly with the administration of the place they live. This in turn can help to include public opinion in planning processes and democratise the design and management of urban spaces (Macintosh, 2004).

Taking all of the above into account, it is difficult to assess the usefulness and impact of these interventions as a whole. While elaborate measures of harm and police demand may give some indication of the usefulness of these interventions in terms of crime prevention, they largely ignore the overall usefulness across other realms (Greenfield & Paoli, 2013; Ratcliffe, 2015).

3.8.3.2. Predict

Predictive policing is in itself nothing new and has in the past grown to become one of the most well-researched realms in the field of policing. More recently, however, the wide-scale use of predictive policing has also come under intense scrutiny from both academics and practitioners (Brantingham, Valasik, & Mohler, 2018; Degeling & Berendt, 2017). Whether new technologies can revolutionise current approaches enough to make it a viable tool for policing without compromising privacy and data protection too much remains to be seen. This study has identified eight interventions that sought to provide security services with some form of predictive capabilities (Table 13).

Table 13: Interventions with some form of predictive capabilities

Author (Year)	(Crime) Problem	Solution	Primary function	Secondary function
Noor et al. (2013)	Prediction of situational crime factors	New tool that uses decision support system (DSS) and fuzzy association rule mining (FARM), in which it can extract the factors of situational (opportunity) crime	predict	
Oatley et al. (2015)	Faults of static CCTV	Utilising CCTV as a sensor to accurately model or give feedback on the reality of occurrences in digital space	predict	
Castelli, Sormani, Trujillo, and Popović (2017)	Growing amounts of data	AI system for predicting violent crimes in urban areas starting from socio-economic and law-enforcement data	predict	
Garg et al. (2018)	Street crime	Gain insights into historical crime data to predict crimes	predict	
Catlett et al. (2018)	Forecasting inefficient	Predictive approach based on spatial analysis and auto-regressive models to automatically detect high-risk crime regions in urban areas and forecast crime	predict	
Isafiade and Bagula (2017)	Street crime	Crime series pattern detection	predict	
Araujo, Cacho, Thome, Medeiros, and Borges (2017)	Robbery and homicide	Smart city platform aimed at integrating several information systems from law enforcement agencies	predict	integrate
Kagawa, Saiki, and Nakamura (2018)	No information about crime in nearby area	Analyse street crimes according to users' living area using personalised security information service. Output is a crime map that helps citizens to avoid crime areas.	predict	warn

The extent and scope of these capabilities varied, however, greatly between the different interventions and reached from more traditional uses of historical crime data (Catlett, Cesario, Talia, & Vinci, 2018; Garg, Malik, & Raj, 2018; Noor et al., 2013) to the detection of psychopathy and potentially dangerous behaviour through CCTV and agent-based simulation through friendship networks on social media platforms (Oatley et al., 2015). What is new about many of these interventions is that their predictive capabilities include the real-time analysis of data as well as mechanisms for subsequent resource allocation, i.e., actuators. This separates them from current predictive policing tools which have been criticised for not being more accurate than an experienced police officer.

In addition, the growing importance of the online realm is reflected in a growing number of approaches. The model introduced by Oatley et al. (2015) emphasises that many people no longer express themselves actively in urban spaces but rather online, and that surveillance systems scanning crowds for suspicious behaviour only see half the picture (Oatley et al., 2015). This not only adds social media as a new dimension of urban surveillance, but it also forces a fundamental change in how we think about and plan for urban security.

3.8.3.3. Section Summary

This section has introduced various interventions with functions that are not, or only to some extent, currently in use in policing and crime prevention. As such, they do not correspond to traditional functions of security interventions. While many of these interventions certainly offer great potential for transforming safe city designs and urban security landscapes, it is hard to evaluate the extent to which they will impact urban security as a whole due to the fast-paced nature of technological development. In addition, a lack of deployment cases and evaluative studies makes it impossible to predict what side-effects they may have (Siregar, Syahputra, Putra, & Wicaksono, 2018).

3.9. Chapter Summary

Our review introduced three categories of security interventions in smart cities. While some of the examined interventions did correspond to the traditional functions of security interventions both as sensors and actuators, this chapter proposed a new classification for smart security interventions based on their functions.

Our classification distinguishes between three main categories, each with two sub-categories. The first category focussed on those interventions that combined new sensors with traditional actuators. This included interventions to detect and prevent unwanted criminal behaviour, and those aimed at identifying, authenticating, and defeating offenders. The second category included those interventions that sought to make old systems smart by either improving/automating processes or by managing and integrating the interplay between existing security solutions. The third category entailed those interventions that introduced entirely new functions such as (mass) information and crowdsourcing as well as threat or crime prediction.

While this classification can help to group and compare interventions, they can also be useful to explore the distinct set of opportunities and challenges that they bring about. The proposed classification highlights that not all systems need to be fundamentally new to become smart and that building on existing infrastructure is crucial for a successful smartification. In addition, the analysis presented in this chapter emphasises that the implications of the deployment of new security technologies in urban spaces are far-reaching with regards to urban planning and governance. Throughout, this chapter demonstrates that future security infrastructures are not separate systems but reliant on and a prerequisite for the deployment of smart systems across other realms of city services. Especially the latter is important to consider for future smart city planning. Instead of treating security and crime prevention as the cherry on top of any smart city development, urban planners should consider it as a foundation. Not only do safety and security significantly impact if and how citizens interact with urban spaces but as shown in the discussion above, there are a variety of tools that can be used for citizen engagement across different realms of city services.

Overall, it is important to remember that smart security measures and the concept of the safe city are not born from the overwhelming failure of existing interventions but rather from the wish to improve existing efforts and to make them more efficient and manageable in the future. As such, they should be seen as a part of a larger holistic system that offers opportunities across all realms of city administration.

These opportunities do come, however, at a cost. The far-reaching deployment of smart technologies brings about new ethical considerations as well as implications for the planning process itself. Questions of data ownership and privacy rights grow in importance and need to be reflected in contemporary planning processes. This chapter highlighted the importance of discussing these issues and criticised the lack of attention they have received in the smart city debate.

The question remains whether the use of such technologies will undermine individual privacy needs in the long run. Some authors stipulate that "surveillance technologies are a key component of smart and networked cities preventing or detecting crime and giving the residents a sense of safety" (van Heek et al., 2016), while others such as Oatley et al. (2015) go as far as to describe CCTV networks as the fifth utility in smart cities. Yet while many innovations might create more efficient city services or effectively reduce crime, they might at the same time make people feel less secure because they have a sense that 'Big Brother' is watching. Particularly in authoritarian (or at least not fully democratic) regimes, the deployment of these new security measures can exponentially increase state power and control over its citizens. There is thus significant tension, as yet unresolved, between issues connected with these new technologies, especially with regards to privacy and data protection, and the importance of urban surveillance and security infrastructure for providing safety and security in the 21st century city.

Chapter Four

Innovation in Practice: Interviews with Practitioners

4.1. Chapter Overview

This chapter examines what challenges practitioners face in the procurement, deployment, and use of crime prevention and detection technologies. The issue is explored through twenty expert interviews conducted with practitioners in London between August 2019 and March 2020. This study expands previous more theoretical literature on the topic by adding a practical perspective and advances the understanding of issues faced in innovation processes and their management.

The study identifies variety of issues and challenges to technological innovation for policing. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public-private partnerships, and public acceptability. While individual practitioners may have the expertise and willingness to unleash the full potential of surveillance and crime reduction technologies, they are usually restrained by institutional rules or, in some cases, inefficiencies. In terms of the latter, this study especially highlights the negative impact of a lack of technical interoperability of different systems, missing inter- and intra-agency communication, and unclear guidelines and procedures.

The results presented in this chapter have also been published in form of the following journal article:

- Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. International Journal of Police Science & Management. DOI: https://doi.org/10.1177/14613557211064053

4.2. Introduction

Technology has become prevalent in most areas of society and, in a struggle to keep up with recent advances, public agencies are forced to innovate at an ever-increasing rate. The use of technology has, however, been an important part of police work, and technological innovation has gone hand in hand with the evolution of police practice (Borrion, 2018). Improving effectiveness and efficiency to keep up with growing demand while remaining within tight budgetary constraints is a core driver of this symbiotic relationship (Chan, 2001; Laufs et al., 2020b). Moreover, the 'entrepreneurial revolution' has increasingly left many organisations involved in policing internally scrutinised by management systems and internal audits and externally under the eye of 'watchdogs', public complaints systems and central auditors. Chan (2001) goes as far as to suggest that 'technology has redefined the value of communicative and technical resources, institutionalised accountability through built-in formats and procedures of reporting and restructured the daily routines of operational policing'. The effect of technological innovation on organisations can vary depending on the nature and the design of the technology and the way in which change is managed. The impact of information technologies is considered to be especially substantial, as officers increasingly cannot complete their tasks without them (Chan, 2001). Smart cities could radically change how police operate, similar to the impact of successfully implemented predictive policing technologies (Sandhu & Fussey, 2021). With additional challenges brought on by the COVID-19 pandemic, the overall dependence of police on technological innovation to improve their operations increased manifold (Azoulay & Jones, 2020; Laufs & Waseem, 2020).

Today many police forces are more 'tech-savvy' than ever before (National Police Chief's Council, 2016). In recent years, there has been an empirical turn in policing driving the increased use of advanced technologies to document, inform, and assess police decision making (Sandhu & Fussey, 2021). The aim of technologically enhanced police work is to make analysis and decision-making more objective and to avoid human subjectivity and bias (Bachner, 2013; Bennett Moses & Chan, 2018; Karppi, 2018; Perry, 2013).

With industry standing ready to satisfy this appetite with crime analysis software, drones, and body-worn cameras, amongst others, there is an increased use of technological products (Higgins, 2016; McQuade, 2006; Rogers & Scally, 2018). This development is not hard to understand since both crime and policing co-evolve with technology in what Ekblom (1999, 2005) has called an 'arms race'.

Because this is such an important issue for the future of policing and crime prevention, it is not surprising to see public and academic discussions on this topic. However, these are generally dominated by a focus on theoretical and philosophical aspects of technological innovation in the field. With the overwhelming focus on the implications for the wider society, there is limited research approaching the topic from practitioners' perspectives and discussing the impact on those who actually use those technologies. This is echoed by Sandhu and Fussey (2021) who find that practitioners' perspectives are often under researched, especially in the field of predictive technologies. Overall, there is a lack of insight into the experiences of the users of smart SOSTs, including the operators, who might take drastically different roles in smart systems. This study helps fill this gap by addressing the under researched area of what knowledge surveillance operators and police officers have about new SOSTs and how procurement and deployment processes work.

In doing so, it specifically focusses on the use of so-called SOSTs, which refers to all technological solutions aimed at detecting or preventing crime by gathering data and monitoring citizens (Pavone & Esposti, 2012). While not all new security technologies are surveillance-oriented, the term is still useful as a large proportion of technologies for crime prevention and detection include, or rely on, some form of monitoring or sensing component (see Chapter 3). The most commonly known form of a SOST is arguably closed-circuit television (CCTV) which is implemented widely across London and the UK (Dixon, Levine, & McAuley, 2004). As such, innovation and deployment of new CCTV systems and the improvement of existing (and possibly more intrusive systems) are a key focus of this research. In addition, other technological solutions (both software and hardware) are considered that may support police in overcoming operational challenges in their day-to-day activities. Here, however, a special focus is placed on smart devices and those aimed at automating tasks.

Similar to many other police forces in the UK and around the world, police and crime prevention services in London have faced austerity and budget cuts over the past decade with severe detrimental effects across almost all areas of activity (Brown, 2020; Greig-Midlane, 2019).

At the same time, London is at the forefront of digital transformation and modernisation and on the path of becoming a 'smart city'. Briefly defined, this term means any city that uses new information and communication technologies to improve the wellbeing of its citizens and make services more resource-efficient (Elmaghraby & Losavio, 2014). This also includes improvements to citizens safety and security and, as such, by default, police and surveillance in the city (see Chapter 3). The 'smartification' of the city infrastructure and the rapid deployment of new technologies means that practitioners are confronted with new solutions but also new problems on a daily basis. A large part of this process are the aforementioned SOSTs and the deployment of technological solutions to tackle resource insufficiencies.

To explore the practitioner perspectives and the practical issues encountered in the procurement and deployment of new SOSTs, a series of expert interviews were conducted with 20 London-based senior crime reduction practitioners. Their views were elicited about the utility of smart and emerging digital technologies for crime prevention and detection and specifically SOSTs. Further questions probed the challenges that are most likely to impede effective procurement and operation. Specifically focused on a group of stakeholders underrepresented in the literature (Liu, Lu, & Niu, 2018), this study offers a glimpse into practitioners' perception of smart infrastructures. The findings contribute to a richer picture of SOSTs in smart cities and their future use and inform the ongoing debates on their likely risks and benefits.

In the following, this chapter discusses why technological innovation is necessary and how the debate on policing and surveillance is often one-sided. Then it lays out the methodological foundations before identifying and discussing the themes emerging from the interviews.

4.3. Background

4.3.1. Innovation and Practitioner Perspectives – Beyond Theoretical Issues

The first important question to answer is why focussing on practical issues of the deployment of new SOSTs and especially practitioners' perspectives is important. While discussing overarching and often philosophical issues of security vs. privacy and questions of individual rights is crucial, it rarely provides direct insight into how new technologies are actually used on the ground, and therefore perhaps also into the types of outcomes they can be expected to achieve. In many instances, the voices of those working in the field and using new technological solutions in their daily work are not part of the discussion when examining issues of surveillance and crime prevention. As such, this chapter does not seek to discuss the broad issues where public discussion often invokes images of a surveillance state and big brother. An example of this is the controversial issue of facial recognition technologies for policing and security purposes. The heated discussion surrounding the deployment of facial recognition at around a large multimodal transport hub in London (Sabbagh, 2019) and trials by London's Metropolitan Police Services between 2016 and 2020 are just the tip of the iceberg (Bradford, Yesberg, Jackson, & Dawson, 2020; Fussey & Murray, 2019). Against this dystopian backcloth of the public debate, academics have been assessing the societal impacts of smart technology and technological innovation in general, often framing them as conflicts between security and privacy or public order and individual rights. In many instances, however, these discussions have neglected the fact that technological innovation can be instrumental in bridging gaps between increasing demand for police services and decreasing public funding. In the last decades, for example, many organisations, including police forces across the world, have initiated a digital 'transformation' (ICT) in the hope of reducing operating expenses and improving service effectiveness, accountability, and procedural regularity (Adams, Baer, Denmon, & Dettmansperger, 2009; Chan, 2001; Crow & Smykla, 2019; Ekblom, 2005; Laufs et al., 2020b; Lum, Koper, & Willis, 2017; Weisburd & Braga, 2019).

This shows that technological innovation in policing and crime prevention is not an obscure scenario in the distant future but rather a necessity that dictates routines and day-to-day activities for practitioners. Indeed, digitalisation and technological innovation play a key role in the Policing Vision 2025 published by the National Police Chief's Council (2016) and the Metropolitan Police Service (2017a, 2017b) which stresses that more must be done to exploit the operational benefits of advances in technology in coming years. This highlights that it is crucial to go beyond the broad philosophical discussions and to explore questions of practical realities in the deployment of new technologies for crime prevention and policing.

4.3.2. Privacy vs. Security – An Outdated Debate?

Public support for crime reduction measures fluctuates over time and often as a result of critical events. Deployment of new surveillance technologies or introduction of new surveillance powers, for example, often occur in the aftermath of tragedies or mass-casualty events, when the perceived need for increased security within the population is the highest (Dinev, Hart, & Mullen, 2008; Thompson et al., 2020) or as a way to cope with otherwise scarce resources by means of automation (Joh, 2019a; Leese, 2021; Wilson, 2019). In contrast, public support is the lowest after data leaks and surveillance scandals such as the Snowden revelations (Hintz & Dencik, 2016; Lischka, 2017; Murata, Adams, & Palma, 2017a).

As a result, the introduction of more technology-oriented security policies and increasingly intrusive SOSTs has provoked two main reactions in most countries, ranging from those who support the increased surveillance in the name of (national) security and efficiency to those who argue that restrictions are undemocratic, unjustified, or plainly useless (Tsoukala, 2006). This dichotomy goes back to the age-old debate of security vs. privacy. Often, this discussion is portrayed as a cost-benefit problem and as a trade-off where one has to choose between security improvements gained through better SOSTs or privacy (Pavone & Esposti, 2012; Pavone et al., 2016).

Several studies examine different angles of this trade-off discussion (Bowyer, 2004; Davis & Silver, 2004; Riley, 2007; Strickland & Hunt, 2005). Nevertheless, pitting privacy and security against each other and viewing the debate as a zero-sum game is far from uncontroversial (Pavone & Esposti, 2012). One important criticism of the framing is that it oversimplifies an otherwise highly complex discussion (Monahan, 2006; Tsoukala, 2006). Furthermore, it deepens the divide between practitioners aiming to improve security and civil society organisations and citizens concerned about their privacy rights. While both issues are important and should work in balance, the way the debate is framed has negative consequences for both sides.

In addition, it is questionable to what extent this debate still applies today and whether it is still timely in its current form. As discussed before, both security and privacy are conceptually shifting. New SOSTs and smart capabilities growingly blur lines between private and public, between volunteered and mandated data. With the rise of the age of data and information, the trade-off between security and privacy becomes increasingly blurry. Today, privacy of one's information and personal data also means security from at least some forms of crime in both the online and offline realm (Braun et al., 2018; Sen, Dutt, Agarwal, & Nath, 2013; van Heek et al., 2017), highlighting the fact that privacy vs. security does not describe a zero-sum game. No rule exists by which one needs to decrease if the other increases. Instead, the example of data privacy in the digital age highlights that both can increase and both can decrease at the same time (Cavoukian, 2009a).

4.3.3. Potential Issues in the Deployment of New Technologies

This study will discuss known issues that can substantially hinder or even stop the use of new technologies in an organisation. For enterprise risk assessment, the ISO31000 (2018) standard distinguishes between *internal* factors (that pertain to the organisation) and *external* ones. In the following, this chapter focuses especially on internal factors as these were overwhelmingly identified by the participants. This section not only provides background about the topic but also lays out a reference frame for the subsequent analysis. The issues and themes discussed herein will guide the analysis and help to contextualise the experiences and information gathered from participants.

A key issue that may occur when deploying a new technology is the impact it can have on the working practices and the working culture within an organisation (Rogers & Scally, 2018). This goes especially for law enforcement environments, with often complex subcultures, as discussed by Reiner (2010). New technologies that promise to change the status quo of individual labour realities can be seen as threatening and potentially rejected by workers (Eugene III, 2001; Hassell, 2006; Nhan, 2014). An example is the introduction of computer-aided dispatch in many US law enforcement agencies in the 1970s and 1980s (Rogers & Scally, 2018). The system was initially widely disliked because of the significant changes it brought to the way police operated. While police agencies have made significant strides in changing attitudes towards new technologies, there might still be some concern, especially in light of the significant potential offered by smart applications and artificial intelligence (Bartsch, 2011).

Another pitfall that might occur when deploying new security technologies is the tendency to impose them on existing structures instead of taking more holistic approaches and ensuring they are integrated into existing systems and can be used to their full potential (Rogers & Scally, 2018). In addition, the use of new technologies in existing systems (both physical and organisational) can lead to the improper use of technologies because they are used to solve problems in the traditional way rather than innovate processes as a whole (Chan, 2001). This is an issue especially hard to tackle in countries like the UK and the US due to the decentralised and, to some extent, fragmented nature of the policing system. While some constabularies might be frontrunners in deploying new technologies, many of the deployed smart technologies cannot live up to their full potential until inter-, and intra-force structures change. This is especially the case in areas such as common databases or county lines where intelligence and information exchange structures between forces often require common standards (Allen, Wilson, Norman, & Knight, 2008; Elliott-Davies et al., 2016; Grace, 2019; Newell, 2013).

In addition, a lack of training and experience in using new technologies can be a significant challenge to the usability of new technologies (Chan, 2001; White & Escobar, 2008). Because urban, societal, and demographic developments do not stop, adequate training is much needed for police to be successful in the future (Taylor, Fritsch, & Liederbach, 2014).

Lastly, especially budgetary and legislative constraints can have a negative effect on the attitude practitioners have towards the deployment and use of new security technologies (Rogers & Scally, 2018). While in some parts, these constraints can be reasonable or even act as important safeguards, practitioners may feel as if they lack support from their superiors or the general legitimisation to employ new technologies (Kirmeyer & Dougherty, 1988).

Much research but also practical evaluations that integrate user focus and usability issues do not make the effort to identify practical user requirements and institutional restraints (Brell, Philipsen, & Ziefle, 2018). Lack of understanding of practitioners' perspectives makes it difficult to improve the usability of new technologies, which in turn can hinder the work of security professionals (Werlinger, Hawkey, Botta, & Beznosov, 2009). This is reiterated by Botta et al. (2007) and Werlinger, Hawkey, and Beznosov (2008) who argue that, in addition to human and organisational factors, technological factors can also have a major influence on professional performance.

Academically, these issues are rarely discussed in terms of security or policing work, especially not with regards to deployment and use of new technologies. This is problematic for two main reasons. Firstly, police work can often set a precedent for organisations with strong and highly intricate group and social dynamics (Hirschmann & Christe-Zeyse, 2016; Ingram, Terrill, & Paoline III, 2018). Secondly, it is a field in which day-to-day operations can significantly change due to the use of new technologies (Chan, 2001). Thus, exploring perspectives of security professionals with regards to the use of new technologies is an important topic that should take a more prominent place on the agenda of policing research.

4.3.4. Why Expert Interviews

The aim of this research was to gain insights into the planning, procurement, and use of new security technologies for policing. Complementing the studies that have analysed policy documents or measure the success or failure of outcomes, this work focuses on practitioners and the issues they faced in day-to-day operations.

Furthermore, official recordkeeping, position papers, or policy documents do not tell much about the precise tactics and strategies of their deployment or capture more informal interactions and processes (Beyers, Braun, Marshall, & De Bruycker, 2014). Another caveat of simple policy analysis lies in the fact that, in some instances, the official position of the organisation may differ from the position of those directly working on the issue (Beyers et al., 2014).

Thus, to understand practitioners' perspectives, this study followed the method proposed by Brell et al. (2018). In their article, the authors carry out qualitative expert interviews to discuss possible use-cases of new technologies and identify benefits and barriers of new traffic monitoring technologies. Other authors such as Beyers et al. (2014) discuss the rationale of interviewing as a data collection instrument in more detail and highlight the merits of it for the purpose of exploratory studies.

Experts can provide 'inside' information that is especially crucial when examining the reality of policy planning processes and day-to-day operations (Dorussen, Lenz, & Blavoukos, 2005). As such, they bridge the gap between single in-depth case studies and large-N comparisons (Dorussen et al., 2005).

4.4. Method

Between August 2019 and March 2020 (pre-COVID), in-depth interviews with 20 practitioners involved in the deployment and usage of new technologies for policing and public security in London were conducted. This section discusses how the experts were selected, the interview process, and the steps taken to analyse the data.

4.4.1. Preparation, Process, and Issues of Validity

Semi-structured interviews were chosen as a method since they offer a balance between the issue-focus of structured surveys and the flexibility of open-ended questions (Dorussen et al., 2005). Interviews were conducted *in situ* to maximise the comfort for the participants and to minimise the strain on their time (Werlinger et al., 2009). In addition, being on-site meant that participants were able to show the interviewer what they were talking about and allowed in several instances for the direct referral of further participants who were working at the time.

Before the interviews, questions were formulated and clustered by theme (Appendix 1). The latter was done to hold the participants' attention and to obtain fully thought-out responses (Beyers et al., 2014; Schuman & Presser, 1996). In formulating the interview questions, academic language, jargon and leading or assumptive statements were consciously avoided (Groves, Singer, Lepkowski, Heeringa, & Alwin, 2004). Similarly, open questions were prioritised in order to allow stakeholders to freely express their views.

4.4.2. Recruitment and Participants

Population boundaries were set using Christopoulos (2009)'s seven-question checklist, and only officials and experts working directly with security technologies for public safety in crime prevention or detection in London were considered eligible for the study. The population of interest was not limited to police or those in enforcement capacities but included those working with CCTV, e.g., councils and other public officials. Involving those working with CCTV was considered appropriate as it has become a mainstream crime prevention strategy in many countries around the world (Piza, 2018) (see Chapter 2).

To find participants, this study used the peer-esteem snowball technique (PEST) presented by Christopoulos (2009), which combines network analysis, snowball sampling, and elite interview methods to confidently construct pseudo-representative samples of experts. Not only did this reduce the risk of selection bias, but it also helped to take into account network boundaries, provided an estimate of the population size, and allowed for clustering of expert opinions on the basis of their nomination network. As such, applying the technique contributed to addressing known weaknesses of snowball sampling, including selection bias, population clustering, and the difficulty to motivate expert participants, as discussed by Erickson (1979).

In an initial step, gatekeepers to the expert population were identified (Christopoulos, 2009). While PEST suggests using a number of unbiased informants, this was not applicable to this case as the pool was already restricted through the limited number of public institutions working in the field. In a second stage, participants were asked to provide further nominations in a series of snowball waves. In this sense, some of the interviewees were accessed through senior 'gatekeepers', and as such might be considered key informants, i.e., individuals who were knowledgeable and experienced about the use of surveillance technology in the police service. The generic stages of PEST are outlined in Table 14.

Table 14: Generic stages of PEST (adapted from Christopoulos, 2009)

	1st Stage	2nd Stage	Subsequent Stages	Final Stage
Primary Scope	Selection of seed nominators	Approach first wave nominees	Approach all new nominees and non-respondents	Reach population saturation or significant sample size
Validity Considerations in Expert Interviews	Estimate the degree of fragmentation of the population and include all sub-clusters of experts.	Non-response bias. Authority of sponsoring organisation affects non-response. Centrality within the sub-clusters of nominated actors.	Approach individuals who have not responded.	Unlikely to reach saturation. Sampling may not sufficiently capture diversity of views. Not a good instrument for capturing dissent.

Interviews with security professionals present several challenges (Botta et al., 2007; Kotulic & Clark, 2004). Practitioners often do not have time to participate, may not be willing to disclose sensitive information, and there is often no publicly available contact information (Werlinger et al., 2009). In order to overcome these challenges, professional connections were leveraged to find initial contacts.

Sampling dimensions included the participant's role within their organisation as well as their level of seniority (Bartsch, 2011). Table 15 gives an overview of the (anonymised) participants along with their affiliation and position within their organisation.

Participants were grouped according to their affiliation and professional role. Affiliations were either policing organisations or CCTV control rooms[10]. Professional roles included participants with management and planning duties, as well as officers who conducted day-to-day policing operations on the ground (e.g., patrolling) or generally those working directly with security technologies for crime detection and prevention in their daily work. Including both, those with and those without management responsibilities in this study allowed for a broader spectrum of experiences and thus a more comprehensive insight into the dynamics surrounding the deployment and use of new technologies. The exact affiliations of the participants (see Table 15) could not be disclosed due to confidentiality reasons.

Table 15: Affiliation and role of participants

Affiliation[1]	**Senior Leadership**	**Frontline Practitioners**
CCTV Control Rooms	3	3
Police	7	7

[1]For confidentiality purposes, all participants are anonymised.

4.4.3. Interview Protocol

In total, 20 experts were interviewed, varying from one to seven experts per organisation. Each interview lasted between 30 and 60 minutes. This qualitative approach produced rich data that was subsequently analysed using a systematic approach (Halperin & Heath, 2017, p. 279; Miles & Huberman, 1984).

While the interviews did not ask for sensitive information *per se*, the first participants who were interviewed requested for their answers not to be recorded. As a result,

[10] Noteworthy is also that the CCTV control rooms are not run by police forces but by local authorities. While their primary function is detecting crime and securing evidence (through video recording), they also operate to monitor other factors such as traffic.

this study followed the example by Chong (2008), meaning that detailed notes were taken and specific quotes were written down during the interviews. These notes were then transcribed and revised shortly after the interviews, as suggested by Beamer (2002). Upon completion, the interviewing notes were discussed with the interviewees to ensure accuracy and awareness of the interviewer's works (Bryman & Cassell, 2006).

While this approach was not ideal and recordings would have provided a range of benefits[11], the study followed best practices from the literature. In fact, the literature suggests that such an approach delivers comparable results with regards to data quality to directly recorded interviews with few drawbacks (Rutakumwa et al., 2020).

Nevertheless, this also means an increased role of the researcher in the recording of the data resulting in a need for increased sensitivity to the significance of the researcher for the research process (reflexivity) (Bryman & Cassell, 2006). In other words, the increased involvement of the researcher in the data collection and interpretation process (i.e., the taking of notes as opposed to simple recording) increases the implications of the researcher in the generated data (Bryman & Cassell, 2006). Defending such an approach, Rutakumwa et al. (2020) write that "choosing not to use an audio recorder […] should not be viewed as a weakening of research conduct but rather as a successful indicator of the researcher's sensitivity to the integrity of the research project."

Interviews were only conducted if participants provided informed consent to take part in the study as per the UCL ethics regulations.

4.4.4. Coding and Analysis Method

To analyse the rich data, the detailed interview notes were synthesised, and common themes were identified (Huberman & Miles, 2002, p. 10). The coding frame was not

[11] For a more in-depth discussion of benefits and drawbacks of different data recording methods in interviews, we recommend Hayes and Mattimoe (2004).

purely derived from the data itself but rather the previously defined research questions were used to shape the analytical lens (Halperin & Heath, 2017, p. 279). This helped reduce the amount of data to process and allowed for a more efficient extraction of the most important and meaningful parts. Setting a predefined coding frame made it easier to summarise patterns of similarities and variability better and identify differences between the different groups of participants. The study maintained enough flexibility to explore the explanations given by the participants in more depth (Glaser, Strauss, & Strutzel, 1968).

Responses were broken down into single statements that were then clustered around common concepts and themes. This was done iteratively within each interview, and related statements were then grouped together (Appleton, 1995; Bartsch, 2011). In addition, this study organised statements based on the participant's position within their organisation. This made it possible to determine whether responses to a single question differed between participants of different levels of seniority or affiliation.

The analysis followed the pattern of clustering answers within the following four categories: (a) what knowledge practitioners had about recent technological developments, (b) what benefits and issues experts could identify with regards to these new technologies (e.g. benefits to their day-to-day work), (c) what challenges they had previously and were likely to face in the deployment and use of new security technologies, and (d) what they would emphasise in the design of new security technologies. In the following, each theme will be discussed, and the responses pertaining to it analysed. The analysis also reports some of the comments that were discussed by only one or two experts but that were found to be particularly useful in thinking about the use of new security technologies or generally representative of the consensus amongst experts.

4.5. Results

The presentation of the results is structured around the interview topics to allow a better overview and easier comparability when replicating this study in other settings. Not only does this section give insights into the most important findings but also the lack thereof in some of the categories. A contextualisation and evaluation of the importance of individual results along with the resulting implications follow in the subsequent discussion.

4.5.1. Knowledge of Practitioners

This first category of questions served to assess the participants' knowledge, categorise their responses to other questions and ensure that answers were given on the basis of a sufficient knowledge base (Halperin & Heath, 2017, pp. 288-291; Tourangeau & Smith, 1996). All but one participant demonstrated knowledge about new security technologies and smart cities. The participant that did not have much knowledge in this area was retained because of their role within the Metropolitan Police Service. The concrete technologies mentioned ranged from smart streetlights to autonomous cars and parking, as well as the use of smart drone technology and urban surveillance.

> *"I know about smart streetlights and smart parking" – Police*
>
> *"It is happening increasingly. They recently started a smart city initiative in my area" – Police*
>
> *"As police, we need to go with the times. My smartphone has great capabilities, and I think we could really use better technology to improve police work" – Police*

All participants confirmed that they had acquired this knowledge in a work-related context, with one participant stating that they had to *"[…] constantly evolve in order to stay ahead"*. Participants were also able to describe situations in which they had previously encountered the deployment and use of new technologies. They were able to recount numerous examples from their professional and personal lives, and many were up to date with regards to new technological innovations and smart capabilities.

4.5.1.1. Differences Between Groups

Overall, answers were largely homogenous, with all participants demonstrating knowledge of new security technologies and, at least to some extent, about smart cities. Despite the rather homogenous knowledge demonstrated by the participants, the specific technologies that each practitioner recounted heavily depended on their work. Though all participants were asked the same questions about their knowledge of new SOSTs and smart cities, their interpretation of these terms was highly subjective. No further explanation or clarification was given at first in order to avoid priming the participants. While many CCTV operators described SOSTs, including the use of wireless mobile cameras, sound surveillance as well as smart street lighting systems, police officers described primarily wearable devices or new technologies for patrol vehicles.

> *"Mobile camera units can help us with watching new hot spots and to see whether we need permanent cameras" – CCTV*
>
> *"We could really use something like [smart] glasses that allow us to see an augmented version and information of the suspects" – Police*
>
> *"[We need] a mobile tracker to point us in the right direction when on foot" – Police*

This divide, however, was not only seen horizontally between participants from different organisations but also nuanced depending on the level of seniority within the same organisation. While frontline participants and operators recounted practical interventions to help in day-to-day operations, participants who worked in management positions often interpreted the question to include technologies for personnel management and more efficiency-improvement tasks.

4.5.2. Benefits and Issues

The second set of questions aimed to discuss which benefits and issues practitioners identified with regards to new security technologies and what impact this could have on their day-to-day operations. Two themes emerged from the stated benefits: efficiency and effectiveness. Besides these, practitioners described operational concerns, but they did not mention issues of social acceptability or privacy risks to the same extent.

4.5.2.1. Benefits for Efficiency

The first sub-theme of efficiency emphasised that the bottom line of all innovation should be to make police work more efficient and to reduce administrative and staffing work.

> *"Clocking in and out from a shift should be digital. Sometimes we start our shifts before, for example, if we come to help with an incident before clocking in. A digital system would make this much easier" – Police*
>
> *"Especially for managing staff and the organisation we need better digital systems" – Police*

The participants almost unanimously agreed that a key priority should be to reduce the time individual employees spend on non-crime related tasks. All of the participants in the CCTV control rooms noted, for example, that they were often understaffed and faced a growing workload of requests from both public and private bodies. Though one might argue that most public bodies are always underfunded and short-staffed (Barnes & Henly, 2018; Vinod Kumar, 2014), interviewees were able to give very specific examples in which this became a security issue. One participant working in a CCTV control room noted that

> *"While at high times four staff are on watch, this is often reduced to two. This means that [the control room] is often understaffed, and operators have to complete multiple tasks at once."*

Conditions like these are problematic in terms of the occupational health of the operators (Laufs & Waseem, 2020) but also a threat to public safety and crime prevention if there are too many incidents for operators to respond to (Rankin, Cohen, Maclennan-Brown, & Sage, 2012). This is a known problem and has been identified in the literature before (Keval & Sasse, 2010). As a result, participants suggested that smart technologies would offer new avenues to cope with the workload and help optimise staff performance. They especially highlighted automatic video classification and person/video re-identification as promising tools for the future. Both technologies refer to the use of AI to automatically classify the content of video data (Boukerche et al., 2017; Brezeale & Cook, 2008).

Another advantage that operators saw in technology was that maintenance and troubleshooting could be improved as most software issues could be fixed remotely and only required one call to the company running the system. This advantage, especially prevalent in cloud-based systems (see e.g.Valentín et al., 2017), meant that lengthy repair processes could in many cases be foregone and issues of data storage and loss to a large extent ruled out.

4.5.2.2. Issues of Interoperability

Participants stressed that the deployment of new technologies had downsides too:

> *"If we get a new system, it won't work with the existing ones." – CCTV*
>
> *"We got a new system to manage staffing and clocking in and out, but it did not work and was not as flexible as the way we did things before, so we stopped using it." – Police*
>
> *"We have a brand-new communication system, but we cannot use it because some of the other agencies are not on the same system." - CCTV*

The most common issue named by the participants was that new and old systems were often incompatible. Many described day-to-day practices in which new systems did not match existing interfaces and thus were not usable. Participants reported that this slowed down their work significantly. Not only did software and integration issues make single tasks harder, but they contributed to a less productive and more tense work environment.

> *"Everyone got annoyed because we had to use the new system, but it took much longer than how we did things before" – Police*

Even the installation of new hardware elements such as cameras was not always straightforward. One CCTV operator recounted how the procurement of new cameras had been highly problematic because they were not compatible with the current software and that the procurement of new software was pricey and much discussed within the organisation. The participant lamented that there were no larger studies exploring the feasibility of new features or which software would be most sustainable in the future. Because the subscription to new software was too expensive, an interim solution was decided, and old cameras were integrated into the old system, which ultimately limited their functionality. Though the academic literature proposes some solutions to this problem, such as customisable plug-and-play solutions (Baldoni et al., 2017), they rarely reflect the realities of CCTV control rooms as bottlenecks of multi-agency collaboration. Proposals of single system architectures or platforms for smart interventions as proposed by de Diego et al. (2018) or Valentín et al. (2017) are thus often hard to set up under real conditions.

Compatibility issues are present even in the more modernised CCTV control rooms. In contrast to the first CCTV control room visited by the interviewer, the second control room had just undergone a complete refurbishment. The entire borough had been equipped with 70 new high-definition cameras, and additional smart technologies such as smart lampposts[12] had been rolled out. The security-

[12] Smart lampposts use sensors to adapt the lighting to the flows of traffic and pedestrians in order to reduce electricity usage, minimize costs, reduce maintenance and CO2 emissions, and enhance public safety and wellbeing (Dizon & Pranggono, 2021). Their utility can go far beyond lighting as smart lampposts can include video monitoring devices, air pollution sensors, RFID readers,

relevant data from all of these smart interventions converged in the control room, but despite the modernisation efforts, compatibility issues were still prevalent. While the borough had updated all its systems, the aforementioned bottleneck meant that several other agencies such as police and other emergency services had communication channels to this control room. Here, the radio used to keep in touch with the police was older than the other systems and, as such, not compatible. While the new digital phone system was able to connect different stakeholders simultaneously and could log incidents automatically, the old radio system only worked one-to-one.

> *"A very annoying problem […] that despite the investments and modernisations we cannot use the new radios because they are not compatible with the ones the police give us. Now we can only wait till they get on the new system and even then, we won't know if it will be the same." - CCTV*

Similar issues were reported by the participants who worked for the police, with some stating that the installation of new patrol car tracking systems had *'disturbed their routines'* and *'cost lots of time'*. As such, participants showed themselves generally open to the installation and usage of new technologies but were critical towards those that were meant to replace larger parts of the system or had too much of an impact on their daily operations. While there was no general rejection of new technologies, some practitioners were disillusioned by the new systems that had been put in place. This issue is in itself not new as already two decades ago, Chan (2001) urged that technologies for policing must be compatible with those of other agencies.

emergency call buttons or charging ports for electric vehicles (Babu, Nisha, Dhasan, Venkatesan, & Karthikeyan, 2021).

4.5.2.3. Benefits for Effectiveness

The focus of this study does not solely lie on CCTV. While those participants working immediately with CCTV (3) primarily described technologies to make their work more efficient, it was police officers who identified technologies with the aim of making crime prevention and detection more effective.

> *"It would be very useful to get something to find suspects and where they live faster. Maybe even see who lives at a certain address or whether they are there." – Police*
>
> *"It would be very useful to be able to see someone's criminal history before approaching them" - Police*

Those in management positions were very conscious of potential benefits for staff allocation and budgeting, whereas frontline participants focussed primarily on how technologies could help them identify and apprehend offenders. Within the latter group, CCTV operators placed a larger emphasis on analytical capabilities, police officers clearly highlighted communicative and mobility technologies. Participants stressed that currently, prevention programmes were not reaching the right people and that they would have to *'get in their channels'* to make programmes more effective. In contrast to this, the question of whether this would affect personal liberties and the extent to which some suggestions could be considered invasive was not much discussed. This was partly due to the fact that there were no established structures and that these issues would have to be discussed on a political rather than an operational level.

4.5.2.4. Issues of Social Acceptability

Though many of the technologies identified and discussed by the experts have undeniable benefits, issues of ethics and social acceptability were only little discussed as potential drawbacks. This could be attributed to a range of reasons (e.g., practitioners' perspective on the issue or their perception that this was not a topic the interviewer wanted to hear from them), but it nevertheless brings up questions with regards to the ethical deployment and usage of these technologies. Most of the practitioners stated that while they were involved in procurement decisions, assessments of social acceptability and possible ethical drawbacks were not up to them. Instead, participants recalled how these issues were 'up to the politicians' (CCTV) and rather 'strategic and political decision' (Police) instead of practical ones.

Only one expert, one of the control room managers, stated that the local council had considered *'systems with AI and facial recognition software'* but had been *'scared off by a possible backlash'*. This indicates that issues of social acceptability can have a great impact on the acquisition process, with interventions deemed too risky not selected.

4.5.3. Institutional Challenges Faced by Practitioners

4.5.3.1. Deployment at the Cost of Existing Systems

One of the biggest challenges that practitioners identified for the deployment and use of new technologies was that the practical impacts on their work were often not sufficiently considered in the procurement and deployment process.

> *"We had a system that worked well, but that was replaced. It would have been better to spend that money on something else" – Police*

> *"It made our work much harder because everyone had to get used to the new interface and the way it worked. It made it much more difficult" - CCTV*

Another example of this is the response from one practitioner about the re-design of a CCTV control room which was moved out of a shared building with the local police unit and into a third location in an effort to streamline police services and increase CCTV capabilities. This re-design of the control room was not discussed with operators or middle management, a fact that was heavily criticised by the participant:

> *"It made it much harder to communicate with the police because before, they were in the same building and would just come upstairs. Now we have to call them or email them, and it takes up much more time."* - *CCTV*

As a result of the move, operators had less contact with the police and more work with administrative processes (such as writing emails or phone calls) that would previously have been addressed in person. While new software was bought to make work in the control room more efficient, it was quickly rendered useless as it was incompatible with other systems used in the control room and by other agencies.

Another participant reported that a new shift management system for the police station causing severe delays in people clocking in and out as it did not allow for the needed flexibility in working hours. While both moves were meant to improve efficiency and lower the administrative workload within the organisations, they ultimately increased the amount of paperwork and labour needed to deal with problems.

This study suggests that these negative impacts and unintended consequences were, to a large extent, limited to the use of efficiency-oriented technologies, i.e., those aiming to reduce administrative work and increasing productivity.

Though most organisations may go through a transitional phase, the cases described by participants indicated more severe structural issues as unintended consequences (see also Chan, 2001; Patel et al., 2018). The current study also found a sharp discrepancy between the answers provided by frontline practitioners and those with management responsibilities. The latter emphasised the positive effect of new technologies in managing their workforce and accomplishing their job, the former often highlighted the negative impacts and unintended consequences of the deployment of new systems. While this had to do with their respective roles, it indicated at least some disconnect between managers and frontline participants.

4.5.3.2. Financial and Political Commitments

Within the police as well as the CCTV control rooms, managers were interested in deploying and using a variety of new technologies to enhance efficiency and effectiveness.

> *"We are already behind with digitalisation. We need to do better." – CCTV*

> *"There are not many projects where this is not discussed. It seems to be everywhere now, so we try to use it to make things better" - Police*

However, participants identified a lack of political commitment and financial support as significant challenges, especially with regards to the use of smart surveillance systems and more far-reaching and comprehensive approaches. One participant formulated his disagreement like this:

> *"[Politicians] don't want to put all of their eggs in one basket. They make small commitments rather than large ones that would bind them in the future."*

This echoes the concern that several practitioners did not feel fully supported in their roles by their superiors and the institutions they worked for. In many cases, the use of new technologies was not governed by clear regulations. The resulting ambiguity led to frustrations amongst many practitioners.

4.5.3.3. Public-private Partnerships

Practitioners identified the interaction with private partners such as private security companies, real estate developers, and private land/building owners as potential challenges. This was especially the case in scenarios where private entities limited the control of police or where crime prevention and policing depended on their approval or cooperation.

> *"On one hand, we need to work with them, but they also can become a headache" – CCTV*

> *"There is a lack of communication between them and us, and they usually use their own systems instead of relying on us" - CCTV*

Participants working in the control rooms stated that especially rapidly constructed new developments were growingly becoming a problem for existing CCTV infrastructure. Newly planted trees obstructed cameras, and many new developments rather relied on private CCTV services that did not allow access to their cameras. This created more and more 'blind spots', which intensified issues such as person or vehicle re-identification. As a solution, the participant suggested that increased dialogue between developers and CCTV would be needed.

Issues with this regard were exclusive to participants working with CCTV and those remotely controlling surveillance technologies. They also mentioned that while the deployment of a new communication system with local security guards had been set up to reduce the workload of police, it had only increased the workload for control rooms where more and more lines of communication converged.

4.5.3.4. Social Acceptability

Lastly, several practitioners identified either implicitly or explicitly social acceptability[13] and the public's trust as a limiting factor.

> *"We have to be careful what the public think we do with this" – Police*

> *"There is a lot of debate, and we want a system that works and not something controversial" - CCTV*

Especially participants from the newly renovated CCTV control room mentioned that while more advanced surveillance technologies had been considered before the modernisation, only a few had ultimately been deployed. Practitioners in this control room stated that they

[13] It is to note that this was not discussed as an ethical or moral dimension but rather as a practical concern for the procurement and use of new technologies.

> *"had to reject a few [surveillance technologies] because of financial reasons. They were simply too expensive. […] we could not do most of them because people would not have liked it."*

Participants from the police made similar suggestions, stating that public acceptability of the technologies would be a significant challenge and that people would consider many interventions to be an invasion of privacy. However, none of the practitioners were able to provide specific metrics that were or could be used to evaluate how the public felt about a certain crime prevention or detection tool.

Even though some participants referred to public opinion surveys on facial recognition and other more advanced technologies (see e.g.Bradford et al., 2020; Bromberg, Charbonneau, & Smith, 2019; Fussey & Murray, 2019), they highlighted that there were no specific surveys for each individual case they referred to. This means that while social acceptability and the view of the general public can hinder or even fully stop the deployment and use of new crime prevention and detection tools, the threshold for this is often arbitrary and rarely follows an evidence base.

4.6. Discussion and Recommendations

This chapter identified a variety of issues and challenges to technological innovation for policing and the deployment of new SOSTs. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public-private partnerships, and public acceptability. The following discussion groups and contextualises these findings, highlighting the most important ones and laying out implications for further research as well as recommendations for improving innovation practice in the field of security and policing. The section first discusses the institutional and technological foundations needed for technological innovation before examining discrepancies and synergies between the academic debate and practice, especially with regards to issues of social acceptability and ethics.

4.6.1. Institutional and Organisational Requirements for Successful Innovation

The expert interviews conducted in this study indicate that there are two possible issue areas that need to be examined specifically when troubleshooting technological innovation in policing. These include institutional foundations and organisational support to enable practitioners to work effectively and technological coordination and interoperability.

With regards to the former, this research found that practitioners are often more open-minded and eager to increase technological innovation than initially assumed. If solely considering the general characterisation of security practitioners and police in the literature as usually not one of tech-savvy individuals, such a result would have been unexpected (Sheng, Kumaraguru, Acquisti, Cranor, & Hong, 2009; Werlinger et al., 2009). Many of these studies are, however, decades-old, and this research finds that those working with technologies today are often not only knowledgeable in their field but seem to keep up to date with trends and recent developments.

Nevertheless, there is a significant amount of scepticism, and many practitioners believe that technologies would make their work more difficult in some respects. Despite this, many interviewees suggested that they were in favour of increasing innovation and were actively bringing in ideas.

One important take-away message is that there is a lack of institutionalisation of technological innovation in policing. Strict hierarchies and inflexible structures create bottlenecks for innovation that make bottom-up innovation often impossible and can reduce the effectiveness of top-down innovation (Borins, 2002). Instead, efficient leadership and institutional structures that allow innovation are needed to enable both top-down and bottom-up initiatives. This includes political leadership that provides clear rules and regulations but does not interfere with day-to-day operations (Borins, 2002).

In several cases, participants felt that they did not have the support of their superiors for deploying or using smart technologies to the fullest. This disconnect may indicate a challenge to effective change management (Campbell, Brann, & Williams, 2003; Hirschmann & Christe-Zeyse, 2016). A lack of support from superiors can have several negative effects on the motivation of staff and the overall work environment (Kirmeyer & Dougherty, 1988). Insecurities felt in the (middle--) management of an organisation will inevitably translate into the lower ranks, which can severely hinder the widespread deployment and use of new technologies and ultimately foster a general rejection of them, as described by McQuade (2006) or Chan (2001). The findings of this study echo those of Sandhu and Fussey (2021) who explore practitioner perspectives on predictive technologies, finding that many were aware of the technologies' limitations, making them more reluctant to use them. Pushing new technologies on practitioners without proper consultations and without evaluating the impact on day-to-day activities may create a backlash and resistance from those working with the technologies. This is also described by Sandhu and Fussey (2021) who describe how resistance against predictive policing technologies turned a technology meant to aide police in their daily operations into an 'arena for contestation and negotiation'.

This creates a circle of problems which hinder innovation, as especially with limited budgets and increased public attention, political support and budgetary commitments come under increased scrutiny, and decision processes become longer (Abramovaite, Bandyopadhyay, Bhattacharya, & Cowen, 2018; Schmidt, Philipsen, & Ziefle, 2015). As such, this project suggests that clear guidelines are needed that emphasise coherence in dealing with technologies and discourage managers from undermining organisation-wide initiatives directly or indirectly.

It is important to note here that throwing technology at the problem is not an answer, as studies such as the one by Garicano and Heaton (2010) find that the use of new technologies alone has neutral and, at worst detrimental effects on police productivity, if not accompanied by appropriately flexible organisational and management practices. This is further supported by the findings of Mastrobuoni (2020) that suggest the success of technological innovation depends largely on the surrounding institutional framework. Moreover, this supports the notion that social environments and technology have a mutual impact on one another, which is the focus of the field of Science and Technology Studies (Hackett, Amsterdamska, Lynch, & Wajcman, 2008; Woolgar & Lezaun, 2013). While a full analysis of this interplay of social environment and technology goes beyond the scope of this research, it is touched upon in several respects of this doctoral work.[14]

Change is often wanted by police forces and other agencies but rarely institutionalised. This is problematic as innovation (especially technological one) does not exclusively bring about benefits but also unexpected drawbacks. A lack of standardised processes and the capacity of practitioners to foresee such drawbacks is therefore problematic (de Diego et al., 2018). Because public agencies are often not set up to follow the fast-paced, dynamic environment that technological innovation requires, many practitioners stated that they were faced with bureaucratic challenges in almost all of their actions, not only restricting their ability to do their job but also negatively impacting their work morale. Frontline participants working for the police suggested, for example, that tools for demand prediction and management would be useful to streamline organisational structures and free up resources. While demand is extremely difficult to predict, some tools exist to make or at least improve predictions (Borrion, Kurland, Tilley, & Chen, 2020; Boulton, McManus, Metcalfe, Brian, & Dawson, 2017; Davies & Bowers, 2019; Laufs et al., 2020b). While the increased automation of processes and the technologization of day-to-day tasks might be able to make operations more

[14] On the one hand, questions of how technology shapes human behaviour (which becomes especially clear with the example of surveillance) are discussed (Graham, 2005b; Klauser, 2021), on the other hand, especially Chapters 5 and 6 focus on the question of societal conditions for technology acceptance and the social construction of technology (Norris & Armstrong, 2020).

efficient and cost-effective, some authors point towards possible downsides in terms of effectiveness, when experienced officers are cut out of the equation (Joh, 2017a).

In many instances, practitioners voiced concerns about the chronic need for additional staff and resources. Though one might argue that a lack of funding is a common frustration, especially in public agencies, that does not necessarily advance the understanding of their view on the procurement and deployment of new SOSTs, this is not the case. A key aim of this chapter was to explore practitioner perspectives on technological innovation in their organisations and the priorities when procuring and deploying new SOSTs. The aforementioned frustrations with resources and financing were often mentioned and should thus not be discounted but rather seen as an important part of the practitioner perspective.

Working conditions as those described by some of the practitioners are problematic in terms of the occupational health of the operators (Laufs & Waseem, 2020) but can also constitute a threat to public safety and crime prevention if there are too many incidents for operators to respond to (Rankin et al., 2012). This is a known problem and has been identified in the literature before (Keval & Sasse, 2010).

This and the fact that budgetary and resource constraints were so often mentioned highlights the need for new technologies to manage increasing workloads and more diverse ranges of tasks in times of austerity and shrinking resources. Especially with even tighter budgetary constraints as a result of the COVID-19 pandemic, public agencies will need to embrace innovation to manage resource shortfalls and maintain effectiveness (Azoulay & Jones, 2020). Nevertheless, practitioners also saw potential in the use of new technologies to deal with resource shortages and staffing problems. This echoes the findings by Wilson and Weiss (2014), who examined how individual staffing and individual workload can affect policing operations.

4.6.2. Interoperability of Systems and the Way to Smartness

In addition to the lack of support and institutional structures to enable effective work, practitioners also identified technological issues that were hindering progress. This included specifically the interoperability of systems both between those of different providers and between different agencies.

This was a common theme across all participants, regardless of their level of seniority or affiliation was that new solutions should be compatible with existing systems or, as one participant put it: 'new technologies should be fluid and should piggyback on what is already there.' This echoes the findings by several authors, such as Datta and Sarkar (2017) and Patel et al. (2018), who propose that, especially in a public context, systems compatibility should be prioritised. This issue is in itself not new as already two decades ago, Chan (2001) urged that technologies for policing must be compatible with those of other agencies.

Though the academic literature proposes some solutions to this problem, such as customisable plug-and-play solutions (Baldoni et al., 2017), they rarely reflect the realities of CCTV control rooms as bottlenecks of multi-agency collaboration. Proposals of single system architectures or platforms for smart interventions as proposed by de Diego et al. (2018) or Valentín et al. (2017) are thus often hard to set up under real conditions.

This study recommends thus a more coordinated and collaborative approach to ensure interoperability and harmonisation of systems. This is especially important in the context of future smart cities, where the fragmented deployment of smart technologies can have significant impacts on their usefulness (Fernandez-Anez et al., 2018; Libbe, 2018). Chmutina and Bosher (2017) repeatedly emphasise the importance of a holistic approach to smart infrastructure, especially with regards to security. Even though the literature discusses this issue primarily with regards to achieving broad coverage of smart technologies across a city, the examples above give insights into the potential side effects on a micro-level (i.e., the effects of just one change to one office).

In addition, the results indicate that issues with private stakeholders lead to increased inefficiencies in the new systems, which echoes the findings of Liu, Mostafa, Mohamed, and Nguyen (2020b). Issues of public-private partnerships are not new (Cvrtila & Perešin, 2014; Purtova, 2018), but they are more relevant than ever in the context of smart cities, for instance, as future urban infrastructure is likely to be increasingly privatised (Liu et al., 2020b). Most models of the smart city rely heavily on the harmonious interplay of private and public agents and on the mutually beneficial use of each other's infrastructures (Ankitha et al., 2017; Choi & Na, 2017). To foster such a mutually beneficial relationship, this research suggests an inclusive forum encouraging relevant stakeholders to take a more unified approach to crime prevention and the deployment of smart technologies in an area, as suggested by Borrion et al. (2019).

4.6.3. Ethical Concerns and Social Acceptability

The findings also indicate a disconnect between practitioner needs and those issues dominating the public discourse on the matter. At the same time, however, ethical, and normative debates are necessary to maintain a balance in the procurement and use of new SOSTs.

While individual practitioners may have the expertise and willingness to deploy SOSTs to their full potential, they are usually restrained by institutional rules and regulations (or, in some cases, inefficiencies). Indeed, practitioners are bound to codes of practice and their actions limited by laws and guidelines in order to ensure no actions are taken unlawfully (Germain et al., 2011). As such, this form of restraint is a crucial and reassuring element of a functioning security system in a liberal democracy. However, once legal and ethical requirements are satisfied, practitioners also face the issue of social acceptability when deploying new crime prevention and detection technologies. Because the evidence base on this is still insufficient and because many organisations rely on arbitrary thresholds, it is hard to overcome or even define the challenge social acceptability presents.

As a result, considerations of this nature are often only a minor and not institutionalised part of SOST implementation processes. This may, of course, be attributed to the fact that procurement decisions and considerations of such nature are made by policymakers rather than those operating or working with the technologies directly. Though this separation of those directly involved in the use of surveillance and those making procurement decisions is essential in a democratic society, it brings about several issues for both sides of the equation. While most practitioners are likely proponents of the introduction of more advanced SOSTs rather than scrutinising ethical or acceptability concerns, limiting their involvement in the procurement decision to merely practical issues can be problematic. Ethical considerations and also those of social acceptability need to be made when examining the full picture instead of selective opinion snapshots. Here, further research is needed to explore the interplay between day-to-day practice and overarching ethical issues.

This is also highlighted by the before-mentioned concerns about resource constraints which not only present practical challenges to policing and surveillance but are an important part of the ethics debate. If the budgetary situation is too dire, practical needs may outweigh ethical concerns or those of social acceptability (Pavone & Esposti, 2012). At the same time, those deploying SOSTs might consider their use ethical and proportionate because they are in control and proportionality of surveillance is always relative (Macnish, 2014). This means that leaving ethical considerations up to NGOs and privacy rights groups and operational concerns to practitioners pits these groups against each other in a struggle to win political favour either for or against the deployment of a new system.

Police rely on an ethical and socially acceptable deployment of new SOSTs as strong opposition to a new technology has the potential to harm police-community relations and trust in police (Bradford et al., 2020; Neyland, 2006). Thus, a better approach would be to engage with both groups and search for acceptable solutions that satisfy ethical standards just as much as operational needs. This echoes the findings of several previous studies, suggesting that more inclusive and nuanced approaches that highlight issues of function creep, data commercialisation, discrimination, or privatisation of data are needed (Amoore, 2006; Côté-Boucher, 2008; Liberatore, 2007; Lodge, 2007b; Spence, 2005). Overall, a more distinct evaluation process is needed that includes various perspectives and leaves room to find a compromise. This chapter suggests that the gap between the practical needs of practitioners and socially acceptable and democratic solutions needs to be bridged by further research and active engagement of citizens by the government.

4.6.4. Limitations

While expert interviews were considered the most appropriate design for this study, there are still some limitations. Though, in theory, it would be useful to increase the sample size, the pool of potential experts on this matter is limited on a local or even national scale. As such, significantly increasing the sample size was not a feasible option in the case of this research.

Because not all experts are equally knowledgeable and may make mistakes, the data is admittedly, to some extent, more diverse and 'messy' than in other modes of research (Dorussen et al., 2005). This, and similar issues of (inter-) expert reliability are often not extensively discussed in much of the current literature, and it is crucial to at least acknowledge them (Dorussen et al., 2005; Halperin & Heath, 2017; Hooghe et al., 2010).

Other issues of validity could be disregarded altogether. Issues such as time-lag between the interview and the topic or events in question were not relevant in this case since this study aimed to explore the professional opinion and experiences of stakeholders, factors that would likely not change significantly over night (Beyers et al., 2014).

4.6.5. Future Research Questions

This research was useful to explore the practical concerns of practitioners about the procurement and deployment of new SOSTs and other smart technologies, however, it also brought up a range of new research topics that should be addressed in subsequent studies.

Firstly, while this research suggests that police as an institution is often too stiff for the growingly fast-paced technological developments, additional research is needed to understand exactly which institutional dynamics should be changed to increase flexibility and allow for better technological innovation in the police.

Secondly, future research should pick up the findings regarding the arbitrary threshold for social acceptability and the lack of established procedures. This is essential as social acceptability is an essential prerequisite for the success of any new policing technology (Bradford et al., 2020). In addition, a lack of acceptance by the public can not only impact the intervention in question but may have a lasting negative impact on police-community-relations as a whole (Nam, 2018).

Thirdly, the question remains whether the results of this study can be seen as indicators of a "smartification of policing'? While the answers to the first background question were mainly used to categorise the subsequent responses, they also helped to put findings into the context of the existing literature. Experts had knowledge of technologies and did not show any direct dislike of their deployment or use. Though this may be expected given most individuals work directly with technology in their day-to-day work, it stands in contrast to previous findings and the general characterisation of crime prevention practitioners and police in the academic debate. Though this sample was too small to tell much about the wider organisations, it would be interesting to identify, through further research, the extent to which we can observe a technologisation or even smartification of policing.

Lastly, this research uncovered possible detrimental effects of increased privatisation in the field of public security and surveillance. It further suggested that the distinct lack of institutionalised measures and the reliance on external agencies hinders technological innovation and prevents police forces from staying up to date. Here it would be useful for further research to examine the individual steps in public procurement processes and identify opportunities for streamlining them.

4.7. Chapter Summary

Overall, this chapter identified three key areas for improving current practices of procuring and deploying new surveillance technologies for policing and crime prevention in London. Firstly, institutional setups need to be made more flexible and conducive for (technological) innovation. This includes increasing support from policymakers and leaders, as well as regulatory clarify for the deployment and use of new SOSTs.

Secondly, this chapter highlights issues of interoperability as current but also future challenges to the use of SOSTs in policing and crime prevention. Here, not only technologically compatible systems should be procured but their deployment should also take practitioner concerns into account to minimise disruptions in day-to-day operations.

Lastly, this chapter highlighted the current lack of guidelines and evidence with regard to social acceptability. More research is needed to provide a better evidence base for future deployments of new SOSTs. At the same time, evaluation processes should be formalised and made more inclusive to ensure issues of ethics and social acceptability are not overshadowed by budgetary constraints and resource shortages.

These results only partially corroborate the findings of previous studies or the characterisation of police and crime prevention practitioners in the literature and, as a result, have several implications for the academic debate on technological innovation in policing and crime prevention. The theoretical discussion often highlights ethical issues and those of social acceptability, even though – in the interviews at least – most practitioners discussed these as rather peripheral issues in the procurement and implementation of new SOSTs. Instead, practitioners focussed on functionality and direct impacts on effectiveness and efficiency in their daily work.

The main implications arising from this are that the academic debate needs to place a greater focus on practitioner perspectives and operational and practical issues. This can be done by involving practitioners and those working with SOSTs on a daily basis more and emphasising the importance of ethical and socially acceptable deployment from the onset of the procurement process (Azoulay & Jones, 2020). The overall lack of research reaffirms the urgency of this project. Not only is it important to evaluate the social acceptability level of individual interventions, but the findings of this study also indicate that there is a practical need for general criteria to evaluate to what extent the general public will examine a specific intervention.

Chapter Five

Exploring Social Acceptability: Characteristics of the Intervention

5.1. Chapter Overview

This chapter examines the issue of social acceptability, taking a closer look at the effects of a range of factors on the social acceptability of a deployment of new SOSTs in the UK. The chapter aims to answer the question which characteristics (intrusiveness, level of automation, effectiveness, location) impact how socially acceptable a new surveillance technology is.

The results are based on a vignette-based online survey that was conducted in early 2021. By examining the characteristics of the intervention itself, this study provides a starting point to evaluate future developments and develop policy recommendations for the future procurement and deployment of SOSTs in the UK. The results of this study are examined in Chapters 5 and 6. As such, method and study design are only discussed once. Together with Chapter 6, this chapter adds to the conceptual understanding of the complex dynamics surrounding acceptability and helped to visualise how different factors contributed to it. Especially within the frame of smart cities, this is novel and has to some extent an exploratory character.

5.2. Introduction

In the UK, surveillance technologies such as cameras have become part of the urban landscape and it is hard to imagine airports, train stations, banks, or department stores without them. Often, they are seen as an integral part of crime prevention and a common measure to protect urban and public spaces from anything ranging from vandalism and terrorist attacks. The deployment and expansion of surveillance technology is often justified by its ability to improve crime prevention as well as the high levels of acceptance within the wider population. As for the former, a variety of studies have examined the crime prevention effect, largely concluding that it is conditional and only applies to certain offences under some conditions (Armitage, 2002; Cuevas, Corachea, Escabel, & Bautista, 2016).

With regards to the second, much of the literature shows that the acceptance of surveillance technologies such as CCTV is high throughout most populations in Western Europe (Krempel, 2016; Kudlacek, 2015). As mentioned in the introduction, especially after terrorist attacks or other significant events that reduce public resistance, surveillance capabilities are expanded, a process the literature dubbed 'surveillance creep' (Fussey, 2007). Examples from the media demonstrate, however, that the use of some technologies does cross the line and provokes protest (Bradford et al., 2020; Sabbagh, 2019).

This means that there is a stark difference between the use of ordinary closed-circuit television (CCTV) and so-called SOSTs that have smart or otherwise expanded capabilities (Nesterova, 2020) when examining their public acceptability. Adding to the already highly complex and context-specific nature of social acceptability research, which means that exploring it requires specialised and focused studies that examine use cases in detail (Bramley, Brown, Dempsey, Power, & Watkins, 2010; Nam, 2019).

While in the past 20 years, numerous scientific articles have repeatedly ascertained that the acceptance and effect of (video) surveillance has not been adequately empirically explored (Goold, 2005; Hempel & Bittner, 2007; Sousa & Madensen, 2016; Zurawski & Czerwinski, 2007), especially after the Snowden revelations, interest in surveillance increased steeply (Adams et al., 2017a; Adams et al., 2017b; Murata et al., 2017a; Murata, Fukuta, Orito, & Adams, 2017b). Today, there is a growing body of literature dedicated to this topic and a reasonable number of empirical studies address the effect and acceptance of video surveillance in public and private spaces (Ditton, 2000; Goold, 2004; Helten & Fischer, 2004; Hölscher, 2003; Reuband, 2001; Saetnan, Dahl, & Lomell, 2004; Thompson et al., 2020; Trüdinger & Steckermeier, 2017; van Heek et al., 2017). Nevertheless, there are still several shortcomings in this field, limiting it both in overall scope and quantity of literature useful for evaluating and improving current practice.

One key problem is that many studies only consider issues of acceptance and acceptability[15] on a superficial level, overlooking the interconnected and complex nature of the concerns people can have (Nguyen, Bedford, Bretana, & Hayes, 2011). In many instances, social acceptability is seen as a black box or a dichotomous condition, when in reality it is likely to be a spectrum that can be influenced by the design of the interventions and demographic factors of the populations that are subjected to the new technologies.

The second major issue is that studies often focus specifically on already existing technologies and contexts where interventions have already been deployed. Though analysing real life situations provides more accurate insights, it means that only little (if anything) can be done to improve the situation in the future and insights for policymakers are likely outdated due to the fast-paced nature of technological developments. In the future, the use of smart SOSTs will likely increase as the smartification of urban environments progresses and increased amounts of data are needed to ensure city services work as intended (Salder, 2020). As such, research that not only considers the current state of surveillance in cities but specifically aims at anticipating future developments is much needed.

While there are some studies examining the characteristics of specific interventions, such as the study by Nissen (2014), they focus often on providing best practices for

[15] Disambiguation of 'acceptance' and 'acceptability': Acceptance refers to the attitude of individuals or groups, i.e., their tendency to evaluate surveillance technologies with some degree of favour or disfavour, after their implementation whereas acceptability means the state of attitudes before the implementation as well as the potential of an intervention to be acceptable (Gärling, Jakobsson, Loukopoulos, & Fujii, 2008; Schuitema, Steg, & Forward, 2010).

the design of socially acceptable technologies. Though these design principles are useful for companies producing the technologies, they neither contribute to improved policymaking on the issue, nor shape governance stakeholder strategies to create a more conducive environment for the successful deployment of new SOSTs.

As a result, there is a clear need for research on the social acceptability of new SOSTs that takes a constructive and nuanced approach while aiming to anticipate future developments and providing concrete recommendations for policy makers. The following chapter will try to address this gap, taking a closer look at the effects intervention characteristics such as intrusiveness, level of automation, effectiveness, and location have on the social acceptability of a deployment of new SOSTs in the UK. The chapter is structured as follows. First, the theoretical foundations of both surveillance and social acceptability are introduced and based on the literature, four hypotheses are developed. Then, the setup of the study and the method are discussed, followed by a presentation and discussion of the results.

5.3. Background

This section introduces the conceptual and theoretical foundations surrounding the use of CCTV and surveillance technologies in general[16] as well as the issue of social acceptability. In doing so it discusses how surveillance and social acceptability can be defined, providing a frame of reference for the subsequent analysis. A special focus is placed on how characteristics of an intervention predict its social acceptability and four hypotheses are developed on the basis of existing research.

[16] While this research does draw a clear distinction between traditional CCTV and new SOSTs, this section refers to both as much of the literature is based on CCTV, but theoretical underpinnings apply to old and new systems alike.

5.3.1.1. Technologies in Policing – A Short History

For decades, the police-related discourse on the use of technology has sought an image that remains unchanged in its basic structure, even if scale and significance of technologies have changed drastically over the years: Offenders (or at least those suspected of offending) use the latest technologies while law enforcement agencies have to make an effort to keep up (Aden; Sousa & Madensen, 2016; Weisburd et al., 2019). With the introduction of cars, for example, the speed at which some criminals could move became a problem for the police. The result was the procurement of faster and newer vehicles for law enforcement (Chan, 2001; Egnoto et al., 2017).

This dynamic can be observed again and again in the history of police technology. The spread of phones led to criminal offences being increasingly planned or carried out with the help of this means of communication (Chan, 2003; Chan, 2001; Custers & Vergouw, 2015; Rossler, 2019). On the police side, this led to the introduction of telephones and early wiretapping (Brownell Jr, 1953).

This relationship between technology used for criminal offences and police technology to counter it, is not limited to transportation and communication technologies and can in some cases lead to a form of arms race between police and offenders (Ekblom, 2017). A more recent example of this is how some countries' police forces have responded to increasingly 'professionalised' terror threats and the online dimension of organised crime, where technical possibilities of avoiding traces trigger ambitions to develop counter-technologies (Kappeler & Kraska, 2015; Roesti, 2020; Salter, 2014).

While technology has advanced significantly over the years, prices for end-consumers have dropped dramatically and as Ekblom (2001) notes: 'Move and counter-move are driven by accelerating change and diffused even more rapidly and efficiently by electronic means or movement of people.' The spread of the internet and advancements in mobile technology have put sophisticated devices in almost every pocket, including those of offenders. Never before have criminals had such a wealth of powerful technology at such a low cost at their disposal (Milivojevic & Radulski, 2020; Tung, 2021).

The question in many counterstrategies is, however, how bureaucratic systems can keep up with an increasingly fast-paced technologization of crime. As early as the 1970s, many police forces began to develop far-reaching plans for a more systematic use of technology (Braga & Weisburd, 2006; Lum et al., 2017; Willis, 2014). What ensued was a steady and unparalleled increase in technological innovation. Processes that previously had to be carried out manually have been accelerated or can now be partly or fully carried out automatically, one example being the comparison fingerprints and biometric data (Aden, 2019).

In addition, safety and security technologies have gained considerable importance both as a research field and as an economic sector. After the terrorist attacks in the US on September 11, 2001, massive investments were made in technology-oriented security research at the state level and in the EU (Levi & Wall, 2004). Today, surveillance and civil security technologies become increasingly important as policing and counter-terrorism efforts are on the forefront of the political agenda and security and surveillance are more closely woven into urban infrastructure (Chmutina & Bosher, 2017).

This revolution does, however, also pose new challenges for police. Investigative efforts related to analogue telephony prove increasingly ineffective. Encrypted messaging services, untraceable digital currencies, and a variety of cybercrime pose new challenges for the police for which no one-fits-all solution exists (Sarre, Lau, & Chang, 2018). This technological challenge is, however, different from advancements in cars or the introduction of phones. Today messaging apps are used by millions around the globe and a breach of encryption by security services or criminals alike might put the privacy and security of all users at risk (Manpearl, 2017). Thus, the stakes in the security vs. privacy debate have never been higher.

'Wiretapping', i.e., breaking the encryption of an encrypted messenger is not only a hypothetical threat to civil liberties but potential back-doors compromise security of all users (Kerr, 2000). As such, a measured and nuanced debate of surveillance opportunities and challenges is needed to anticipate future developments and ensure security, privacy, and justice alike.

5.3.2. Social (Un)Acceptability as a Major Pitfall

One of the biggest issues of the future crime prevention debate is that it is often framed as a purely technological issue. This is, however, not the case, as trade shows, tech publications, and some countries around the world demonstrate again and again. Instead, many governments are deterred by the iceberg of social, economic, political and process challenges that need to be overcome to successfully deploy a new SOST or other technological crime prevention solution (Figure 5). Some of these challenges are more or less easily adjustable as they are purely internal to the government or organisation such as budgetary constraints or a lack of skill within the workforce. Others are highly complex and intricate such as issues of social acceptability. In the following, the concept of social acceptability and possible predictors will be discussed in more detail.

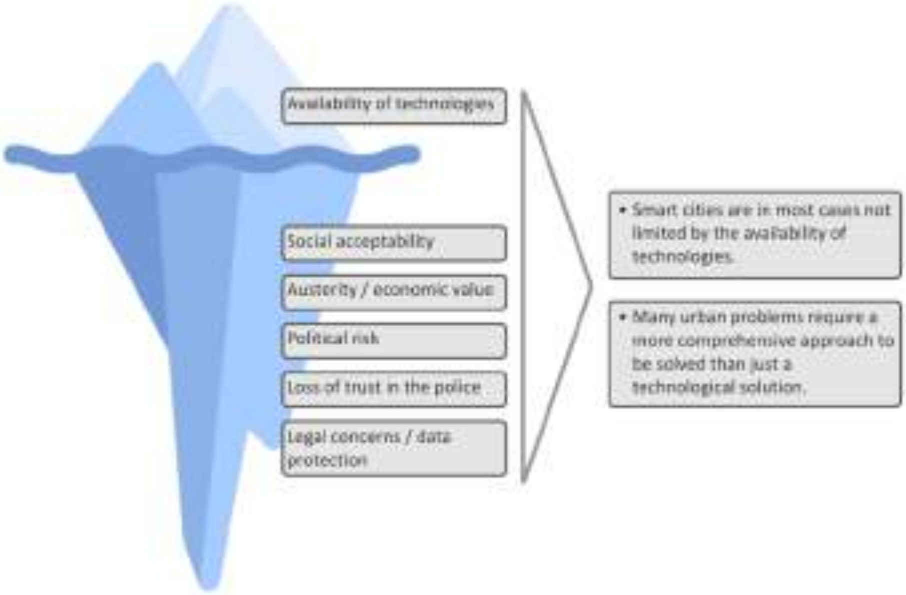

Availability of technologies
Social acceptability
Austerity / economic value
Political risk
Loss of trust in the police
Legal concerns / data protection
• Smart cities are in most cases not limited by the availability of technologies.
• Many urban problems require a more comprehensive approach to be solved than just a technological solution.

Figure 5: The 'iceberg' issues associated with the deployment of new SOSTs in smart cities

5.3.2.1. Social Acceptability – A Theoretical Framework

According to the interaction model introduced by Madensen, Heskett, and Lieberman (2012), individuals acceptance (or support) of a crime prevention intervention depends on four factors. These include (1) the intervention's degree of reasonableness, (2) the extent to which the intervention has a disarming effect, (3) the focus of the intervention, and (4) the consistency of the intervention. Each of these factors can be viewed on a scale from low to high, with citizens more likely to support interventions that generally score highly across the board (Madensen et al., 2012; Sousa & Madensen, 2016). Low scores in only one dimension can cause serious negative effects and a loss of public acceptability (Sousa & Madensen, 2016). The model is based on a number of other theories including Reactance Theory, procedural justice and police legitimacy, Defiance Theory, the Elaborated Social Identity Model, and Differential coercion Theory (Sousa & Madensen, 2016). The model echoes fundamental principles of CCTV and surveillance as tools for crime prevention discussed by authors such as Ratcliffe (2006) and Armitage (2002). In the following, the four principles of the RDFC Interaction Model, reasonableness, disarming, focus, and consistency, will be discussed and a theoretical framework for this thesis developed (see also Table 16).

- Reasonableness of an intervention refers to the appropriateness of the response and the discretionary decisions that lead to the deployment of SOSTs. This factor takes the type and harm of the unwanted behaviour into account and acknowledges that some forms of behaviour or crime are worse than others. Loitering for example may be unwanted but may not warrant an official sanction or deployment of resources. Warnings and action that was preceded by a warning will be received differently by citizens than a zero-tolerance policy. If police action is perceived to be unnecessary or disproportionate, it is likely to face a backlash in the community (Sousa & Madensen, 2016).

- Disarming in this context describes the level of force implied, threatened, or used. This applies to all actions law enforcement take and also includes the deployment of SOSTs. The dimensions of this factor range from non-intrusive and inclusive to highly intrusive and intimidating (Madensen et al., 2012; Sousa & Madensen, 2016). Evidence shows that officers with and without weapons are perceived differently and that overt displays of (physical) power can impact how citizens react to police (Yesberg, Bradford, & Dawson, 2020). In terms of SOSTs and crime prevention measures in smart cities, this especially becomes relevant when examining the design which may, depending on the purpose, be cowing and intimidating or inviting and attractive (Newman, 1972; Nissen, 2014; Poyner, 1983; Schuilenburg & Peeters, 2018). Here, a dichotomy of the smart city environment and surveillance becomes clear. While smart cities aim to maximise quality of life, some SOST interventions (especially those aiming to deter would-be offenders) might only work through displays of power, contradicting much of the smart city agenda.
- Focus of the intervention refers to its scope and the precision with which it can select targets. This applies to both people and places and begs the question whether surveillance technologies by default have to cast a broad net or whether they can become only active when certain (unwanted or illegal) behaviours are spotted (Bourmpos et al., 2014; Wiliem et al., 2012). Sweeping security measures at a large-scale event are more likely to be accepted than in a calm neighbourhood and random spot checks may be seen as arbitrary and discriminatory if conducted at random locations and without consent (Sousa & Madensen, 2016). While some authors suggest that traditional SOSTs are increasingly being challenged by new technologies and AI in order to prevent large-scale privacy intrusions and to maximise resource efficiency (Choi & Na, 2017), others suggest the

opposite, pointing towards the need for large amounts of data by AI and other new technologies (Newell, 2013).

- Consistency means the extent to which the public can rely on the intervention for action when unwanted behaviour is shown. It means the dependability of the intervention and of resulting law enforcement action (Sousa & Madensen, 2016). Delivering consistent results is not only important to ensure crime reduction is permanent but also to build trust within the community.

Table 16: RDFC Model for building citizen support, based on Madensen et al. (2012)

Dimension	Police Response
Reasonable	Protects citizen rights and is appropriate and proportionate to prevent harm
Disarming	Does not use avoidable force, coercion, or intrusiveness
Focused	Targets only individuals, locations, or behaviours that are harming or facilitating harm
Consistent	Is dependable, unbiased, and reinforces behavioural expectations

5.3.2.2. Social Acceptability in the Literature

Hallinan and Friedewald (2012, p. 2) neatly define why research on the public perception and acceptance of government surveillance is crucial. On a more systemic level, they conclude that public opinion should be a shaping factor for public policy in liberal democracies (Hallinan & Friedewald, 2012). This is not only important on a normative level but also because while 'public opinion' is often used to legitimise the use of surveillance technologies there is a significant gap when it comes to understanding how public opinions on the matter are formed. This study seeks to address this gap by examining how specific factors influence the level of social acceptability of a new SOST and making recommendations to support policymaking in the future.

Especially the latter is essential, as public acceptability plays a significant role in policy makers' decision to deploy new SOSTs. A lack of approval from the public can become a significant liability in the cost-benefit analysis that guides future policy

(Pechey, Burge, Mentzakis, Suhrcke, & Marteau, 2014). Furthermore, public opinion is a "shaping factor […] in the development of surveillance technologies and surveillance infrastructures" (Hallinan & Friedewald, 2012, p. 2). Certain technologies are considered to be unproblematic or even simply necessary, while others provoke resistance and outrage. While the latter can in some cases lead to the end of an intervention, citizens may accept it despite their concerns. An example of this is CCTV, which as a rather well established crime prevention and detection intervention in the UK is widely accepted in the population despite some concerns over privacy or the potential for abuse (Dixon et al., 2004).

One of the most influential pieces of research in the debate around the social acceptability of new technologies is the work by Otway and Von Winterfeldt (1982). Already in 1982, the authors saw the potential of social acceptability issues and analysed underlying factors, finding that "opposition to technology is not new and the reasons for it are often complex, often including concerns related to morals, religion, political ideologies, power, economics, physical safety and psychological wellbeing" (Otway & Von Winterfeldt, 1982: 247).

The research suggests that the acceptance of a new technology depends on a number of factors. One fundamental question is for example who conducts the surveillance. In the context of this research, the surveilling body has been clearly defined as the police and government security agencies. This is especially important, as the context of policing shifts the focus of the debate.

Other factors include "the information people have been exposed to, what information they have chosen to believe, the values they hold, the social experiences to which they have had access, the dynamics of stakeholder groups, the vagaries of the political process, and the historical moment in which it is all happening" (Otway & Von Winterfeldt, 1982: 254).

Furthermore, Otway and Von Winterfeldt (1982) defined a list of negative attributes of interventions that lower the social acceptability of a new technology. Their list includes a variety of factors. Those relevant to this study and crime prevention and detection technologies more generally are:

- involuntary exposure to the technology (can individuals opt out?);
- lack of control over the outcome of the exposure (what data is being collected?);
- uncertainty about the consequences (how is the collected data used?);
- a lack of personal experience or knowledge about the technology (what is the technology?);
- difficulty of imagining consequences because of the complexity of the process or technology (often the case with IT);
- delayed or no somatic effects (can consequences appear much later?)
- benefits are not highly visible (why take the risk?);
- the benefits go to others, but the risk to us (unfair to the risk bearers);
- danger of human failure leading to unintended consequences (e.g., data leaks).

Complimentary to this, Otway and Von Winterfeldt (1982) also define a list of attributes which might positively or negatively impact the social acceptability of a technology, depending on how they are weighed by individuals according to their personal beliefs and values. Those relevant to this case include:

- provide a benefit corresponding to perceived needs;
- increase the standard of living;
- facilitate economic growth;
- require strict physical security measures or special police powers;
- increase the power of big business.

Interestingly, research on the acceptability of video surveillance indicates that it rarely correlates with the subjective feeling of security. While in the UK acceptance of CCTV steadily moved towards the 90%-mark, other European countries are not far behind (Hempel & Töpfer, 2004, 2009; Töpfer, 2004). Even in Germany, a country with arguably one of the most CCTV-critical populations in the West often shows approval ratings for the deployment between 50% and 90% (Apelt & Möllers, 2011; Heger, 2010). With the installation of CCTV, however, the subjective feeling of security usually increases only to a much lesser extent, with other measures such as increased lighting or the presence of staff having a much more significant effect (Hölscher, 2003; Kazig et al., 2006; Klocke, 2001). This connection between feelings of security and fear of crime, and the acceptance of new SOSTs will also be further explored in the subsequent chapter in Section 6.5.2.

5.3.3. Predictors of Social Acceptability

Public opinion on new SOSTs can vary greatly between interventions and contexts (Hallinan & Friedewald, 2012). While traditional CCTV enjoys often high levels of approval and is seen as highly acceptable, SOSTs with further reaching capabilities often face backlashes (Thomas et al., 2021; Thompson et al., 2020). In the following this chapter will examine four characteristics in particular, which distinguish more advanced SOSTs from traditional CCTV. Though the list of characteristics tested in this study are by no means exhaustive and there might be many other issues that set new systems apart, this study considers these issues to be some of the most relevant ones in terms of social acceptability. To set a frame for the analysis, the following sections introduce four characteristics which were suggested in the academic literature or derived from real-life examples key features of modern surveillance technologies while at the same time presenting challenges to social acceptability.

5.3.3.1. Intrusiveness

One key characteristic that sets new SOSTs apart, especially in the context of smart cities, from traditional CCTV is the increased amount of data that is collected about citizens. While traditional CCTV only collects visual evidence in the form of video, other SOSTs are far more elaborate and may include functions such as audio recording, various automated recognition tools (e.g., facial or license plate), or even contain components that scrape social media and the digital realm for additional information about individuals (Agha et al., 2017; Datta & Sarkar, 2017; Eigenraam & Rothkrantz, 2016; Qin, Strömberg, & Wu, 2017; Rothkrantz, 2017a). 'Intrusiveness' in the context of this study thus refers to the amount of personal data gathered about an individual.

Real world examples in the past years have demonstrated again and again that the use of such technologies is controversial and increasing the amount of gathered (personal) data can attract severe resistance from citizens if practices are deemed too intrusive (Moraes, Almeida, & de Pereira, 2021; Nesterova, 2020). The trials of facial recognition software in London, for example, revealed that intrusiveness matters and that technologies with new capabilities face greater public scrutiny (Bradford et al., 2020; Fussey & Murray, 2019).

In the case of smart cities, increased intrusiveness is almost impossible to avoid. The data-driven nature of 'smart' innovation means that its success depends to a large extent on the question which data is available and how it has been processed (Bieber, 2018). The large amounts of data are necessary for the functioning of many smart functions and to improve other city services. The gathering of audio data can for example be useful to determine noise levels or sentiments. License plate recognition tools can serve to allocate parking spaces and facial recognition could be part of biometric payment schemes in shops (Moriuchi, 2021). Opportunities for using the wealth of collected data are almost limitless and it is important to consider that the gathering of data is an underlying condition for any 'smart' urban transformation. As a result, SOSTs are likely to gather more data and thus become more intrusive in the future if left unchecked.

Drawing the connection between the more intrusive collection of personal data on one hand and the overt backlashes systems with more capabilities faced in reality, this thesis hypothesises the following:

H1: More intrusive technologies (here CCTV) are less socially acceptable than less comprehensive systems.

To explore this hypothesis, this study distinguishes between two conditions, one describing an 'ordinary' CCTV system only collecting video data and one hypothetical highly intrusive system collecting video, audio, and social media data and employing facial recognition to extract further information. The capabilities of the more intrusive system were designed in order to provide a clear distinction from ordinary CCTV but drew from real-life examples that have been tested and used in different contexts (Givens & Lam, 2019; Leibold, 2020; Schuilenburg & Peeters, 2018; Zenz & Leibold, 2020). Testing such a hypothetical condition rather than a scenario that is closer to reality, may seem counterproductive at first but given the rapid development of new technologies and the deployment of highly intrusive systems in countries such as China, the chosen scenario seems almost tame.

5.3.3.2. Automation

Technological innovation always incorporates some degree of automation (Danzer, Feuerbaum, & Gaessler, 2020). This general rule of thumb applies to both the smart city environment as a whole and security and policing processes in particular (as discussed in Chapter 2). In smart cities, automation is a feature of the way processes and interactions between components are organised (Bayerl & Butot, 2021). In terms of policing, the use of predictive policing tools for example automates the process of crime forecasting and even seemingly minor tools such as new scheduling software can automate processes such as setting meetings or resource deployment (as mentioned in Chapter 3). As such, automation by itself is a natural process and part of modernisation efforts. Police practice wants and needs to be state-of-the-art. Well-trained police officers expect to work on duty at least at the same technological level that has become standard for most people in their private lives, for example through the use of powerful smartphones and computers (Aden; Degeling & Berendt, 2017).

Police ambitions for the use of technical innovations, however, have their limits. Some of these are due to the limited ability to react to new developments as police authorities are cumbersome bureaucratic systems. In some cases, however, such ambitions also come up against legal hurdles, which in a democratic constitutional state necessarily arise from the fact that police use of technology almost always encroaches on basic human rights and civil liberties - with the result that the benefits of the respective technology for the safety of the general public must be weighed against risks to the fundamental rights of those affected and uninvolved (Ferguson, 2019; Furnham & Swami, 2019; Valentino, Neuner, Kamin, & Bailey, 2021). This means that complex tensions between what is technically possible and what is (constitutionally) legally permissible are unavoidable. Political decision-makers are faced with the challenge of having to decide between practical requirements, fundamental rights, and their own political interests (Aden, 2019)

The process of automation itself is, however, not the issue as it is a necessary part of ensuring police forces are ready for future challenges and can manage police demand effectively and efficiently (Laufs et al., 2020b). Proponents of the increased use of smart technologies and AI hope that much of the work previously conducted by humans can at some point in the future be replaced or at least accelerated by machines (Aden, 2019). Nevertheless, automation or in this case the use of AI is a highly debated subject in the field of acceptability research. Many studies explore the effects an increased use of AI has on humans in a variety of settings, often finding that people distrust it (Beiter et al., 2020; Scheuer, 2020a, 2020b). This is in part due to the fact that high levels of automation are often problematised as resulting in 'black boxes' which limit a system's transparency and accountability as well as the possibility for reflective thought (Smith, 2020).

In their comprehensive study, Beiter et al. (2020) find that most people see especially the collection and analysis of personal data by AI as problematic. While the study rejects the common notion that humans will be replaced by AI, it finds that many people are nonetheless critical of the use of AI, especially when they do not understand how the intervention works (Beiter et al., 2020; Nissen, 2014). Their research finds that these critical attitudes are not often followed by critical actions and that especially when the use of AI delivers benefits for individuals (Beiter et al., 2020). Overall, most individuals accept the use of AI unless it was able to take completely unsolicited actions as it could not be controlled to the extent that most people would like (Beiter et al., 2020).

This suggests that the social acceptability of the intervention not only depends on what data is collected but also how this data is analysed and to what extent humans are involved in deciding appropriate action. As such, this study hypothesises the following:

H2: The use of AI that works fully autonomously and can take action without human command for data analysis makes an intervention less socially acceptable.

Automation in the smart city context is generally thought of in the technological sense, i.e., decisions made by machines instead of humans. As such, the hypothesis will be tested through two conditions. The first condition describes the analysis of the collected data by a human analyst, as currently practice in the UK, i.e., a system where critical decisions about the deployment of responses are made by humans. The second condition describes the use of an AI that autonomously and without human input analyses the collected data and takes response measures such as deploying police, sounding alarms, or turning up the lights.

1.1.1. *Predicted Effectiveness*

Beiter et al. (2020) find that the use of AI is considered to be more acceptable when it creates direct benefits for individuals. Thus, this study will examine whether increased benefit would increase the acceptability and thus mitigate any negative effects of the use of fully autonomous AI.

As discussed in the background section, a key function of CCTV and SOSTs in general is crime prevention through deterrence and alteration of the environment. Especially in the context of the smart city, however, surveillance measures and AI are deployed for a range of functions from gathering data to adjust city services and making resource deployment more efficient to preventing crime and increasing individual security (as discussed in Chapter 3). While all of these functions are important, a reduction in crime is arguably the most direct benefit for citizens. In addition, the true value of the SOST in terms of demand and resource management or positive indirect effects is too complex to convey in a brief vignette. As such, this study examines to what extent the predicted effectiveness in terms of crime reduction effects social acceptability of the intervention, testing the following hypothesis:

H4: Interventions with a lower effectiveness are less socially acceptable than those with a high level of predicted effectiveness.

Despite the increasing amount of cameras and the apparent 'internationalisation' of the phenomenon (Hier, 2011), there is still controversy in the academic literature about the extent to which CCTV and surveillance can reduce crime (Sousa & Madensen, 2016) and many authors highlight the possibility of crime displacement (Piza, 2018; Thomas et al., 2021).

Evidence to support the often-suggested crime prevention effect of CCTV and SOSTs in general is sparse (see also the discussion of CCTV in Chapter 2). In their landmark meta-analysis on the effectiveness of CCTV for crime prevention, Piza et al. (2019) find that CCTV is associated with a significant yet modest reduction in crime. The authors note, however, that any effect is contingent on a number of contextual factors such as geographic setting, crime type, camera monitoring strategy, who is doing the monitoring, as well as the use of new technologies (Piza, 2018; Piza et al., 2019). This is echoed by Armitage (2002) who found that timing, seasonal variations, control areas, and possible displacement have to be taken into account when assessing the impact of CCTV. Some studies suggest also that if crime rates fall as a result of the use of video surveillance, as often associated with theft and property crime (Hempel & Bittner, 2007; Khan, Aziz, Faruk, & Talukder, 2020; Morgan & Dowling, 2019), they stabilize again over time or return to their initial level (Kammerer, 2009, p. 76), especially if displacement effects are taken into account.

One of the most comprehensive and detailed evaluations of CCTV as a crime prevention measure was conducted by Welsh and Farrington (2002, 2009). Their study reviews 44 scientific evaluations that met methodological standards for establishing causal relationships (Welsh & Farrington, 2009).

The data suggests that (under certain conditions) CCTV is associated with a decrease in crime of about 16%. While this number is primarily taken from evaluations of CCTV use in UK car parks to tackle property crime, it is echoed throughout the literature with most authors acknowledging the success while maintaining that effectiveness differs across locations (Gill & Spriggs, 2005; McLean et al., 2013; Piza et al., 2019; Ratcliffe et al., 2009; Sousa & Madensen, 2016; Welsh & Farrington, 2009). The crime reduction effect of CCTV or SOSTs in general is not only location specific but also contingent on the crime type most prevalent in the area (Sousa & Madensen, 2016). Evidence on property and violent crimes is mixed (Caplan, Kennedy, & Petrossian, 2011; Gerell, 2016; McLean et al., 2013; Piza, 2018; Piza et al., 2019), while there is more consistent evidence for crime reduction effects with regards to auto theft and disorder (Gill & Spriggs, 2005; Gill & Turbin, 1998; Ratcliffe et al., 2009; Webster, 2009). This is echoed by Armitage (2002), who discusses the evidence on the effectiveness of CCTV in relation to different offense types, coming to the conclusion that the extent to which CCTV can be an effective solution for crime problems depends largely on the context. Because the effect of many of these assumptions is difficult if not impossible to measure or quantify, there is a debate about the usefulness of CCTV. Overall, there is no consensus on the issue of measuring the effectiveness of CCTV. The College of Policing's Crime Prevention Tool Kit (2021) discusses the use of CCTV as a crime prevention strategy in the UK in more detail and synthesises evidence from two systematic reviews to assess the effectiveness and mechanisms through which it works.

While the crime reduction effect of 16% was primarily true for auto theft in car parks (Tilley, 1993), it is used in this study as an anchor point for the effectiveness-measure. Rather than picking an arbitrary number, this study uses this as a realistic baseline in order to make the hypothetical vignette as true to reality as possible. With the assumption that the use of more efficient analytical capabilities (i.e., an AI rather than a human analyst) would also increase the effectiveness of the SOST, high-effectiveness conditions included a projected crime reduction effect of 32%.

5.3.3.3. Location

The placement of CCTV cameras has always been an issue of video surveillance. While in some countries cameras are almost omnipresent, other countries have imposed strict regulations limiting the scope and number of cameras drastically (Krempel, 2016; Reuter et al., 2016; Thomas et al., 2021). As such, location by itself is not necessarily a new factor or one that is especially unique to new SOSTs.

Nevertheless, this chapter argues that it is crucial to include location as a variable due to its future importance. Two developments make the placement of the cameras so important for the social acceptability. Firstly, camera systems are becoming sophisticated and the wide-spread introduction of the 5G network offers opportunities for high quality live-cameras that not only provide higher resolution than CCTV but can also be deployed to cover wider areas (Kim, Cha, Kim, & Kim, 2020; Sugaris, 2020). Where authorities were previously constrained by resources, having to decide where a limited number of cameras are placed, developments such as multifocal technology allow for few cameras to cover over 1000m^2 (Salder, 2020).

Secondly, camera systems that were previously permanently mounted on high poles are growingly being replaced or at least complimented by mobile or even airborne systems that are easy to transport and move around (Dilshad, Hwang, Song, & Sung, 2020; Rao et al., 2020). Both developments mean that the now already often hotly debated issue of location and placement of SOSTs could gain a new dimension. As such, it is crucial to examine what impact location has on the social acceptability.

When discussing the issue of placement and location, the literature gives several insights into why it is such an important consideration (Lang, 2008). Studies suggest that individual attitudes towards surveillance differ depending on whether it is deployed in proximity to one's home or other more frequented places and whether people consider these places to be in need of surveillance (Kudlacek, 2015; Reuband, 2001; Reuter et al., 2016). The latter can be based on objective crime risks or simply the individual perception of victimisation risks, i.e., fear of crime. As a result, fear of crime, previous victimisation, and the crime rates at the place of residence can be important mediating variables when examining the effect of location. If individuals perceive no real threat or generally feel safe in their neighbourhood, they are likely to reject the installation of intrusive SOSTs. People who previously have or live with a fear of being victimised, or those who live in neighbourhoods with high crime rates are likely to accept new interventions more readily. Though this chapter focusses only on the characteristics of the intervention itself, these issues are important to explore which is why they will be addressed in Chapter 6.

In addition, the underlying notion of using location as a variable is that a SOST placed closer to someone's home has a greater impact on their lives. Thus, this study hypothesises that individuals will find more intrusive surveillance less acceptable if installed close to their place of residence.

H3: Interventions installed close to the place of residence of respondents are less socially acceptable than those installed in a random area.

To test to what extent the installation location can predict the social acceptability of a new SOST, this study distinguishes between two conditions in the experiment, one suggesting the deployment close to respondents' home and the other proposing London's Shoreditch as a location. Shoreditch was chosen as it is an area with a busy night-time economy (as also discussed by the vignettes and visualised in Picture 1. It has a high density of bars, pubs, and nightclubs and much of the nightlife happens outside. While London Shoreditch was chosen due to its popularity, effectively, any popular night-life area in the UK would have been suitable, as the sample in this study is UK-wide. Both Shoreditch and the 'home' location were chosen to ensure practical applicability of the research as they are realistic deployment conditions within the UK context.

Picture 1 – Example photo of nightlife in London Shoreditch

5.4. Method

What influence do the before-mentioned factors have on the level of social acceptability of a new SOST? To answer this question, an online vignette-based survey was conducted, which will be discussed in the following. First, the study design and setup will be introduced. Then, the practical statistical approach and analysis methods will be discussed. Lastly, descriptive statistics and in-depth results of the different steps will be presented. As results for both this and the subsequent chapter were derived from the same survey, the study design will only be discussed once.

The study design is founded in a number of good examples from the literature from the fields of social acceptability and public opinion research. The method builds especially on the works of Yesberg et al. (2020), Clothier, Greer, Greer, and Mehta (2015), Reynolds et al. (2019) as well as Pechey et al. (2014).

5.4.1. Study and Vignette Design

The introductory section of the survey gathered general demographic information about participants including age, gender, and ethnicity as well as general information about their previous experiences with police and victimisation. The second section asked about the privacy-related perceptions and behaviours of participants. Then a scenario in form of a vignette was introduced that laid out the deployment of a new SOST in a crime-troubled neighbourhood. Lastly, participants were asked about their attitudes towards the installation of the new system and any concerns they had about it. Acceptability/acceptance always has several dimensions and can also take the form of an adaptation (i.e. in the sense of acceptance) or an adoption (in the sense of an active endorsement) (Kudlacek, 2015). Empirical research should take this into account and should not capture attitudes towards video surveillance based on a single question. As a result, this study measured attitudes towards SOSTs using a scale of multiple items to reflect the multi-dimensionality of the concept of acceptance. Where possible, the items aimed to measure existing constructs based on validated instruments from previously published research or follow best practices of survey design (Table 17). Perceptions of respondents were all measured on a five-point Likert scale.

Table 17: Survey items measuring existing concepts and sources

Construct / Item	Definition	Source
Political spectrum	Political opinion and attitude towards authority	Heath, Evans, and Martin (1994); Kyprianides et al. (2020)
Trust in police / expectation of effectiveness	Level of trust in the police and expectation of how effective police are	Jackson, Bradford, Stanko, and Hohl (2012); Trinkner, Jackson, and Tyler (2018)
Privacy concern general / privacy concern government	Concerns about the use of personal data in general and by the government as well as privacy protecting behaviours.	Otway and Von Winterfeldt (1982); van Heek et al. (2017)

5.4.1.1. Factorial Design

Before final deployment, vignettes and questions were subject to two rounds of piloting. The first pilot was run on 4 February 2021 with two hundred respondents (8 conditions with twenty-five respondents each). The second pilot was run on 8 March 2021 with three hundred respondents (12 conditions with twenty-five respondents each). The pilots were used to refine the questions and test the applicability of the vignettes.

After the two pilot studies, the 'high effectiveness' conditions were added as a variation of conditions 2 and 4 which described a scenario with an AI analyst. This was done as the use of AI in SOSTs is often aimed at improving the effectiveness of interventions. Practically, adding this condition made it possible to test to what extent mentioning increased effectiveness to participants would mitigate any effects of the (hypothetically) less acceptable AI-condition. The final study consisted of a 2x3x2 design, resulting in twelve final vignettes (Table 18).

Table 18: Overview of the final factorial design and its twelve conditions

		Human analyst	**AI analyst**	
	Location	**Normal effectiveness (16%)**	**Normal effectiveness (16%)**	**High effectiveness (32%)**
CCTV	**Home**	1 A	2 A	2 A - HE
	Shoreditch	1 B	2 B	2 B - HE
Highly intrusive system	**Home**	3 A	4 A	4 A - HE
	Shoreditch	3 B	4 B	4 B - HE

5.4.1.2. Vignettes

In the study, respondents were given a brief text to introduce the scenario (Table 19). This vignette described a crime problem as well as the deployment of a new SOST. Each vignette consisted of four core elements that were manipulated between groups. A sample vignette is provided below along with a breakdown of the individual elements. The elements that were manipulated between vignettes included (A) the location of the proposed intervention (close to respondents' home or in an area in London with a lot of night-time economy), (B) the level of intrusiveness (simple CCTV only collecting video or a comprehensive smart system collecting video, audio and social media data), (C) the level of automation (analysis of the data and deployment of response measures either done by a human or an AI), and (D) the level of predicted effectiveness (either a 16% or 32% reduction in crime).

Table 19: Breakdown of a sample vignette used in the study

Vignette Element	Purpose
(A) Imagine you live in a street with several pubs. Recently, there have been increasing disturbances and anti-social behaviour as well as instances of crimes including fights outside the pubs, some theft from cars, and on rare occasions low-level drug dealing happening in the area.	• Introduce the scenario and crime problem and 'setting the scene' for respondents to think about the intervention. • Manipulation element: Location
(B) The police want to address this issue by installing crime prevention technology in the area. The police plan to use CCTV to monitor the area in order to prevent the crimes and to help investigations. CCTV cameras only record video which will be used to identify and gather evidence on suspects.	• Describes the use of the intervention and the amount of data that will be collected. • Manipulation element: Level of Intrusiveness
(C) All CCTV feeds come together in a control centre where they are observed and processed by a human analyst. This analyst tries to detect behaviour that could indicate a crime (such as fighting outside pubs, theft from cars, or drug dealing). If such behaviour is spotted, the analyst will take action. Actions may include deploying police, turning up streetlights, sounding an alarm, or sending an ambulance or the fire brigade.	• Describes the analysis process and consequences of a positive identification of unwanted or criminal behaviour. • Manipulation element: Level of Automation
Expected consequences of the intervention: • Long-term crime reduction of 16% • Short-term increased stop-and-search activity in the area Type of data collected: video	• Summarises the key elements of the proposed intervention and highlights and reiterates the manipulated elements for respondents.

5.4.1.3. Recruitment of Participants

The study itself was hosted on Qualtrics and participants were recruited via the online platform Prolific. Prolific is similar to other crowdsourcing platforms such as Mechanical Turk but has a larger, more diverse pool of UK participants. In line with Prolific recruitment protocols, participants received compensation for their time. This study followed Chandler and Paolacci's (2017) advice on how to minimise participant fraud on Prolific: first, it set constraints so that participants could only take the survey once. Second, attention checks throughout the surveys were included (e.g., questions about the general topic of the survey). Participants were excluded from analysis if they failed attention checks. Nine responses were rejected because they did not correctly complete the required attention check.

To ensure the study was as representative as possible, a pre-screened UK-wide sample that was quasi-representative of the UK population demographics was used. Participants were pre-screened for age, ethnicity, and gender and participation was limited to UK residents. Respondents were asked to type their gender, ethnicity, and age and responses were later grouped together to analyse sub-groups. The survey only included individuals above the age of eighteen. Overall, 1446 participants were recruited to take part in the study. Table 20 breaks down the participants according to demographic factors.

Table 20: Participant Characteristics

		Sample		UK Population 2020[a]
Characteristic		**N**	**%**	**%**
Gender	Male (including transgender men)	702	48.6	49.4
	Female (including transgender women)	736	51.0	50.6
	Non-binary / third gender	5	0.3	0.4[b]
Age range[c]	18-24	139	9.6	7.72
	25-34	271	18.8	16.92
	35-44	239	16.6	15.96
	45-54	263	18.2	16.74
	55-64	327	22.7	15.70
	65+	204	14.1	23.53
Ethnicity	White	1235	85.6	87.2
	Mixed	37	2.6%	2
	Asian	111	7.7%	4.2
	Black	49	3.4%	3
	Other	11	0.8%	3.7

[a] Unless otherwise indicated, all UK Population estimates are based on the ONS Population Estimates Report 2021 (Office for National Statistics, 2021).

[b] Estimate based on an analysis by Practical Androgyny (2021). The percentages in the gender characteristic category are not cumulative as the ONS only distinguishes between male and female.

[c] Calculated based on the total 18+ year old population of the UK in 2020 (Office for National Statistics, 2021).

5.4.1.4. Ethics Approval and Consent

Before taking part in the survey, participants gave informed consent to take part in the study in addition to the consent to take part in research that they had already provided to Prolific. The research was approved by the ethical review board at University College London's Department of Security and Crime Science.

5.4.2. Analysis Approach Summary

Initially, the impact of the experimental conditions (automation, intrusiveness, location, effectiveness) on social acceptability were tested using simple analysis of variance (ANOVA). Other conditions and demographic factors were not relevant at this stage due to the random assignment of respondent to condition, meaning any effect of pre-treatment conditions or demographics should be eliminated (Welsh & Kong, 2011).

In many aspects, this analytical approach follows the example by Liu, Lucas, and Marsden (2020a). The one-way ANOVA and relevant post-hoc tests were conducted using STATA 16 to test whether the differences between the mean acceptability rates differed significantly between the four characteristics (Ostertagová & Ostertag, 2013; Rowntree, 2000).

The analysis was broken down into several parts to simplify the statistical analysis process and to make the results easier to understand. First, the effectiveness condition was removed from the analysis as it was only relevant for analysis within the AI condition, thus leaving a 2x2x2 factorial design with three independent variables, the level of intrusiveness, the level of automation, and the location.

A three-way analysis of variance (ANOVA) was conducted on the influence of the three independent variables (level of automation, level of intrusiveness, location) on the level of social acceptability. All independent variables were coded as dichotomous variables (i.e., present or not present). The results of this step can be found below in Table 21. As in reality, systems would likely include several of the before-mentioned technologies (i.e., be both more intrusive and include AI for analysis), interaction effects were included in the analysis.

After the analysis between the three conditions had been conducted, the standard AI condition (16% effectiveness) was compared to the higher effectiveness AI condition (32%). This was done to test whether an increased effectiveness, would impact individuals' attitudes towards the use of the AI system.

5.4.3. Results

All of the effects in the first step of the analysis were statistically significant at $p<0.05$[17], except for the location factor ($p = 0.319$). The main effect for the level of intrusiveness yielded an F ratio of F (1 , 1,442) = 144.55, $p<0.001$, indicating a significant difference between CCTV (M = 4.02, SD = 1.99) and the comprehensive, highly intrusive system CCTV (M = 3.35, SD = 1.54).

The main effect for the level of automation yielded an F ratio of F (1 , 1,442) = 23.54, $p<0.001$, indicating a significant difference between the use of an AI (M = 3.59, SD = 1.44) and a human analysts (M = 3.87, SD = 1.43). Both the more intrusive and the more automated system yielded lower results than the traditional non-smart system. This was once again confirmed by a Tukey post-hoc test, which revealed that the acceptability of the highly automated (AI) condition was significantly lower than that of the condition with the human analyst (-.284 ± .062, $p<0.001$). Similarly, the more intrusive system was found to be significantly less socially acceptable (-.668 ± .056, $p<0.001$). While there were significant differences between the traditional and the smart and intrusive system, the results still indicate that a majority of respondents found all systems acceptable as all scored above average in terms of acceptability, i.e., over three on a five-point scale. No significant interaction effects could be observed.

[17] There is an ongoing debate about the appropriateness of p-values and their statistical significance. Including a full discussion of the benefits and potential pitfalls of using a fixed confidence level of 95% (α=0.05) goes far beyond the scope of this chapter. Instead, the research followed the practical suggestions by Di Leo and Sardanelli (2020), always reporting true p-values while maintaining the 0.05-theshold to categorise the results or to simplify parts of the discussion where reporting all true p-values would have not resulted in any benefit to this research.

Table 21: Results of the ANOVA

Dependent Variable: Level of acceptability

Source	Partial Sum of Squares	df	Mean Square	F	Prob>F
Model	198.281	7	28.326	25.44	<0.001
Intrusiveness	160.933	1	160.933	144.55	<0.001
Automation	26.208	1	26.208	23.54	<0.001
Location	0.946	1	0.946	0.85	0.357
Intrusiveness * Automation	4.383	1	4.383	3.94	0.050
Intrusiveness * Location	0.130	1	0.130	0.12	0.733
Automation * Location	2.034	1	2.034	1.83	0.177
Intrusiveness * Automation * Location	3.464	1	3.464	3.11	0.078
Residual	1597.665	1,435	1.113		
Total	1795.950	1,442	1.250		

R Squared = .110 (Adjusted R Squared = .105)

In a second test, the automated groups (2A, 2B, 4A, 4B) were compared with groups that indicated a higher predicted effectiveness (2A-HE, 2B-HE, 4A-HE, 4B-HE). This was done to examine whether a higher benefit (here predicted crime reduction) would mitigate negative effects of the use of AI instead of a human analyst. No significant effect of the level of effectiveness on the level of social acceptability could, however, be found (p = 0.623). Table 22 below presents the average acceptability scores in each condition.

Table 22: Average acceptability score in each condition[a]

		Human analyst	AI analyst	
	Location	Normal effectiveness (16%)	Normal effectiveness (16%)	High effectiveness (32%)
CCTV	Home	4.262	3.769	3.902
	Shoreditch	4.313	3.932	3.938
Highly intrusive system	Home	3.354	3.494	3.244
	Shoreditch	3.572	3.231	3.208

[a] Measured on a 5-point scale where 5 = highly acceptable and 1 = highly unacceptable.

5.5. Contextualising the Results – Why Characteristics Matter

5.5.1.1. Intrusiveness

Out of the four tested characteristics, the intrusiveness of the intervention had the strongest negative impact on the level of social acceptability. While this may be intuitive and in fact confirms the hypothesis H_1, it is still a highly relevant finding with implications for the design and deployment of SOSTs.

The CCTV condition was mostly accepted and did not raise concerns with most respondents. In contrast, collecting audio, video, and social media information crossed the line of what is acceptable and solicited a more negative response. This is, however, not to say that the more intrusive system was viewed as entirely unacceptable, scoring still an average over four on the five-point acceptability scale. This indicates that even though respondents found the intrusive system significantly less acceptable than the traditional CCTV system, they still did not reject it but rather found it less acceptable to install.

The reasons for this are complex but the data provides some insights that can help to disentangle these results. Firstly, this study found that most respondents found the use of surveillance both in an intrusive and traditional fashion overall acceptable. This echoes the findings of much of the recent literature, indicating that despite the lack of evidence of its effectiveness, people are generally in favour of more public surveillance to curb crime (Krempel, 2016; Kudlacek, 2015; Reuter et al., 2016; Sousa & Madensen, 2016).

Though the scenario tested in this study may seem extreme at first, there are indeed instances where such systems have been tested or even deployed. China's increasing securitisation and surveillance of Xinjiang Province (Burnay, 2019; Givens & Lam, 2019; Leibold, 2020; Zenz & Leibold, 2020) and its elaborate social credit system which involves the monitoring and analysis of social media are only some examples of where increasingly high-tech SOSTs might lead (Curran & Smart, 2021; Knockel et al., 2015; Qin et al., 2017).

While surveillance measures like in the Chinese context might seem outrageous, dangerous and intrusive to the average European, authors such as Thompson et al. (2020) or Cao and Everard (2008) suggests that individuals living in countries that are high on the power distance index or those from strict hierarchical societies are likely to accept greater surveillance. This highlights that there are differences in what is deemed acceptable not only within a population but also between cultural and societal contexts.

Even when considering CCTV, perspectives differ between European countries. While CCTV is extremely common and well accepted in the UK (as once again highlighted by the results of this study), this is not the case in Germany (Adams et al., 2017b; Möllers & Hälterlein, 2013). In the Spanish context, Adams et al. (2017a) found that citizens are more accepting of government surveillance if they perceive a benefit for themselves or society. Privacy concerns, trust in government and the police, and the perceived need for surveillance are all at least in parts determined by the cultural context (Thompson et al., 2020). The context of national culture is critical when discussing new SOSTs which means that the results of this study are only generalisable to a certain degree and only with the caveat of being tied to a UK context (Thompson et al., 2020).

The finding that intrusiveness of an intervention can be a critical factor in predicting its social acceptability may be universally applicable and useful for the design of new SOSTs. The results do not, however, provide an understanding of exactly which technologies are acceptable and which are not. Here, further research is required with a narrower focus and possibly a comparative perspective to examine the impact in a cross-cultural context.

5.5.1.2. Automation

The level of automation, i.e., to what extent a human was involved in the analysis of the data and the deployment of response measures, showed to have a significant impact on the social acceptability of the intervention. The more automated condition (using the AI analyst) was found to be less socially acceptable than that with the human analyst, supporting hypothesis H_2.

The expectation of proponents of the use of AI is that automated systems are more neutral and freer of bias in their decision making. Governmental entities and police in particular depend on being able to present their actions to citizens and society in general as rational (Meyer & Rowan, 1977). The legitimation of the use of AI can probably benefit from this thanks to the widespread myth of the computer as the embodiment of the ideal of rationality, especially as long as knowledge about how AI work is relatively low within the general population.

At the same time, not many people understand how AI works. This lack of knowledge may mean that some reject AI because they do not understand it or it scares them, thus becoming detrimental to its social acceptability (Klimczak, Kusche, Tschöpe, & Wolff, 2019; Kroll, 2018). AI is often seen as a black box, not only by the general public and lay people but in some cases also by its creators (Rai, 2020). This means that questions remain about how data is stored and used, and it may become hard if not impossible for citizens to understand the inferences and conclusions drawn from the data collected in their everyday activities. This fundamentally goes against the acceptability principles introduced by Madensen et al. (2012) which were discussed in Section 5.2.2.

The 'black box' association may also have contributed to the lack of acceptability in another way. While some may associate the term 'AI' generally with more intrusive data gathering or dystopian scenarios, others may not have any have any opinion or view (positive or negative) but may simply lack knowledge or an understanding of how it could be useful in this context. Respondents were not given extensive information about pros and cons of the use of AI or more elaborate automation in general, meaning they relied solely on their existing knowledge.

5.5.1.3. Effectiveness

The predicted level of effectiveness (in terms of crime reduction) of the intervention did not have a statistically significant impact on the level of social acceptability. This is interesting, as effectiveness is one of the most commonly discussed factors impacting the acceptability of SOSTs in the literature (Kudlacek, 2015).

The value of 16% for the predicted effectiveness was based on findings from previous studies (Armitage, 2002; Cuevas et al.; Moon, Heo, Lee, Leem, & Nam, 2015). The higher value of 32% was chosen as it would mean double of the realistic crime prevention value, i.e., a significant increase. As such, the results do not indicate that effectiveness in general does not have an impact but rather that neither the realistic (and following the literature even slightly optimistic) value of 16% nor a reduction by double would lead most people to show greater support for a more intrusive SOST.

Nevertheless, this means that a proposed benefit such as crime reduction also does not mitigate the negative impact of using AI as initially assumed. Here, it would be interesting to see whether the promise of other benefits could sway individuals to consider the use of AI more permissible.

In addition, it is important to remember that the overall effectiveness of SOSTs is hard to measure and that it relies on a number of passive effects the results of which are difficult to quantify (Armitage, 2002, 2013). Furthermore, effects on subjective feelings of safety also depend on individual experiences and the context in which SOSTs are deployed.

Lastly, anchoring the overall usefulness of surveillance in the total crime reduction fails to recognize that it can also be associated with opportunities. Hölscher (2003, p. 51), who is fundamentally critical of the use of the technology, has pointed out that basically three purposes are conceivable: The surveillance could serve to investigate crimes that have been committed. It could also serve as 'discipline in advance' and thirdly, as it were as a result of the first two contribute to an 'improvement in the subjective feeling of security.' As such, is entirely plausible that SOSTs can have beneficial effects in certain locations and regarding certain offences that are not easily quantifiable in terms of absolute crime reduction (Kudlacek, 2015). Furthermore, there are several benefits associated with CCTV with regards to demand and resource management for police forces (Laufs et al., 2020b). Effectiveness of SOSTs should thus not only be measured in terms of crime reduction. Especially when SOSTs are implemented as part of a wider smart city network, the purpose of surveillance technologies can pertain to other city services (e.g., how many people are in one location could affect how traffic is routed) as well as the overall topic of efficiency.

In summary this means that while the prospect of crime reduction did not have a significant impact, it may be useful to further explore other passive or indirect benefits for individuals through further research. Furthermore, it would be interesting to investigate whether there is a value that would lead respondents to consider interventions more acceptable. While 16% and 32% are more realistic values (one aim of this study), they are admittedly not the strongest manipulation possible and it may be interesting to see whether predicted crime reductions of 50%, 80%, or 100% would yield different results.

1.1.1. Location

Against the initial hypothesis H_4, location was found not to have a significant effect on the level of social acceptability. The first assumption of course is that location simply does not affect social acceptability as respondents either support or reject new interventions, regardless of the location of their implementation.

There are, however, two caveats to this conclusion. Firstly, as already discussed in previous chapters, this study is highly specific to the UK national context as attitudes between regions and countries may differ greatly, specifically with regards to the use of new SOSTs (Banisar & Davies, 1999; Brandl, Frank, Worden, &

Bynum, 1994; Norris, McCahill, & Wood, 2004; van Heek et al., 2017). Other studies in this field have found that placement and location of surveillance technologies, especially in Germany, did indeed have an effect on public attitudes (Bier, 2012; Reuband, 2001). As such, one might hypothesise that location of SOSTs has no effect in the UK context because video surveillance is already highly present in most public urban areas (Webster, 2009).

A second caveat is that the findings only suggest that there is no effect of the two tested conditions (location close to respondents' home/their general area of residence and a more or less random area in London). This means that a stronger manipulation, e.g., by suggesting the deployment right outside the respondents' house may have yielded different results. While the tested conditions are the most realistic scenarios in the UK, other countries around the world are showing that they are far from science fiction (i.e., instances where surveillance technology is installed outside every door) (Leibold, 2020; Zenz & Leibold, 2020).

Two suggestions arise from these findings. Firstly, it would be useful to conduct a further study that more specifically explores the issue of placement of SOSTs and the effect on social acceptability. Here, a comparative study between different national contexts could prove valuable. Secondly, policymakers and police forces in the UK have more leeway in the placement of SOSTs but need to be mindful not to cross certain thresholds. Further studies are needed to determine where these thresholds lie.

5.6. Chapter Summary

This chapter explored how the level of automation, the level of gathered data (intrusiveness), the deployment location, and the suggested effectiveness predict the acceptability of new SOSTs. The analysis found that growing intrusiveness and increased automation both predict a decrease in social acceptability and significantly less favourable attitudes towards the intervention. Even when disregarding cases with severely increased capabilities, comparing the results of this study with those of Reuband (2001) , Hölscher (2003), Bornewasser and Kober (2012) and Bornewasser and Schulz (2008) shows that overall acceptance of SOSTs has decreased, and concerns of privacy and civil liberties have increased over the years. As the aim of this study was not a comparative time-series analysis, these results are only indicative, but a full comparative study over a number of years could prove highly useful to spot future trends and help make more sensible and citizen-focused policy decisions in this field.

Increased automation and intrusiveness predict lower scores in terms of overall acceptability. Despite the relatively lower rating, acceptance of all interventions was overall high. This echoes the findings of Kudlacek (2015), who suggests that the use of smart CCTV is supported by most citizens. While these results are generally encouraging for policymakers and those seeking to increase surveillance in the future, they also have implications for the design and procurement of new SOSTs as well as policymaking. This goes especially for the UK as the results are specific to the national context.

Some research suggests that respondents favour technological solutions over the involvement of human analysts due to the potential for bias and error (Klocke, 2001; Kudlacek, 2015). In contrast to this, this study found the opposite with most respondents favouring human involvement. This may be due to a priming effect through the vignettes, which introduces in some cases highly intrusive and automated systems. While there were significant differences between the conditions, the less-acceptable AI-system was still seen as generally acceptable by most respondents. One suggestion might be to conduct further experiments regarding the use of AI, with a clear focus to increase the efficiency and effectiveness of the new SOSTs.

Though neither location nor the proposed level of effectiveness were significant predictors of interventions' social acceptability, they might still become relevant in real-world cases. As several other studies to point to these factors as significant predictors of surveillance measures (Kudlacek, 2015; Reuter et al., 2016; Rothmann, 2010; van Heek et al., 2017), the absence of significant results may be explained by weak or insufficient manipulation in this study. As such, it may still be worth exploring ways to increase the effectiveness of new SOSTs to improve their social acceptability.

The differences regarding the extent of approval between the different types of SOSTs can also be explained by the somewhat more differentiated recording that was used in the context of the present study. This confirms a view of Zurawski and Czerwinski (2007), who argue that the assessment of video surveillance measures is less positive for more specific and differentiated questions.

Chapter Six

Exploring Social Acceptability: The Importance of Other Predictors

6.1. Chapter Overview

In continuation of the previous chapter, which focused on the characteristics of the intervention itself, this chapter explores external predictors for how individuals respond to the deployment of a new SOST. Using the experimental data from Chapter 5 to explore the demographic factors and sub-groups means that this chapter moves from an experimental paradigm into a correlational one.

The external predictors discussed in this chapter were identified through a thorough review of the literature. Here, the chapter draws from several fields under the broader umbrella of social acceptability of policing or government measures. All variables that are discussed in the previous and this chapter are visually summarised in Figure 6 below.

Ultimately, the chapter seeks to answer a number of research questions. First, the chapter asks to what extent demographic factors such as age, gender, ethnicity, or political affiliation predict the social acceptability of new surveillance technologies. Secondly, it explores how far previous victimisation experiences and the impact of crime on one's life predict social acceptability. Thirdly, it examines the predictive power of previous experiences with and trust in the police before lastly discussing the role of individually held privacy concerns.

6.2. Predictors of Social Acceptability

This section introduces the predictors that were tested in this study. Based on the relevant literature, several hypotheses are developed, which will later guide the analysis. The section is structured around the key factors discussed before and includes a discussion of the importance of demographic factors such as age, gender, and ethnicity.

6.2.1. Political Beliefs

The political attitude of individuals is a critical factor for predicting social acceptability as especially the role of authority in the personal beliefs predicts how individuals may view the use of SOSTs by the government (Hallinan & Friedewald, 2012). Individuals with more right-wing or conservative beliefs, i.e., those with a mindset that values trust in and respect for authority, are more likely to accept increased technological capabilities of the police (Anania et al., 2019) and the use of new SOSTs (Murphy, 2007). As such, the following can be hypothesised:

H_1 Individuals who identify with the political right find the deployment of new SOSTs more acceptable than those on the political left.

While political opinions are certainly a spectrum rather than categorical, the following sections will still refer to them as 'right' and 'left', always relative to the middle of the applied scale. The connection between ideology and concerns about government surveillance may seem obvious. In reality, this nexus is, however, only subject of few studies (see e.g., Dinev, Bellotto, Hart, Russo, & Serra, 2006; Dinev et al., 2008; Lim, Cho, & Sanchez, 2009; Pavone & Esposti, 2012; Smith, 2005) and personal beliefs are rarely referred to as a source of concern or rejection of surveillance technologies (Nam, 2017).

This research gap is addressed by Nam (2017) who discusses the impact of political ideology on concerns about government surveillance. Personal political beliefs deeply impact individuals' outlook on the issue of surveillance and the capabilities the police have. While surveillance does to some extent always impede on civil liberties (Bennett, 1995), it is the reasons for the surveillance and the attitude towards these liberties that drive individual concerns about surveillance (Nam, 2017). In short, this means that while some people might view a surveillance measure as a legitimate tool, others may consider it an 'unacceptable interruption into one's personal sphere', depending on their political beliefs (Nam, 2017).

Nam (2017) suggests that in order to be successful, governments must convey the importance and purpose of the measure to both sides of the political spectrum and educate citizens about their intentions. Surveillance theory and practice should not be black boxes but rather build on citizen participation and input, taking demand and needs of citizens just as much into account as concerns and rejection, especially if municipalities claim the title 'smart city' (Bourmpos et al., 2014; Nam, 2017, 2019). While the ideological classification undertaken by Nam (2017) is not useful for this study, this research nonetheless builds on the overall notion that political ideology is a critical factor in predicting an individual's view on government surveillance.

6.2.2. Victimisation Experience and Crime Impact

Other key predictors of social acceptability include previous victimisation experience and the impact of crime and fear of crime on one's life (Baumer, 1978; Greve, Leipold, & Kappes, 2018; Krempel, 2016; Kudlacek, 2015; Pryce, Wilson, & Fuller, 2018; Reuter et al., 2016). These factors are also important to further explore the results of the analysis in the previous chapter, which found that the location of the new SOSTs was not a significant predictor of social acceptability. This chapter builds on this finding and employs a more nuanced analysis to examine closer to what extent the impact of crime on individuals and previous victimisation experience can predict the level of acceptability of a new SOST.

The underlying idea is that individuals who live in high crime neighbourhoods or whose lives are otherwise impacted by crime in a significant way are more inclined to support the installation of a new SOST. Kochel (2018) for example finds that individuals living in crime hot spots with high risks of victimisation are more inclined to support the police and value effective policing. The study suggests that 'need for help from police promotes police legitimacy' and drives the acceptance of new SOSTs and more capabilities for police (Kochel, 2018). Since surveillance is aimed at reducing crime, it is reasonable to expect that people who fear crime would speak out disproportionately in favour of interventions to tackle it in the hope that this would reduce their own threat.

H_2 Individuals who are more impacted by crime and fear of crime in their daily lives are more likely to accept new SOSTs.

H_3 Individuals who have previously been victimised show greater support for the deployment of new SOSTs.

While victimisation and fear of crime are sometimes discussed controversially, several studies provide findings that support the hypotheses (Kazig et al., 2006; Krempel, 2016; Nam, 2018; Reuband, 2001). The opportunities in the use of SOSTs in high-crime neighbourhoods is demonstrated in the literature (Klauser, 2007; Wheeler, 2016; Wiig, 2018). One example of such an approach is the transformation of Camden, New Jersey, where a new surveillance system with participatory elements (e.g., citizens could watch their own street), served as a key part to decrease crime and support the rebuilding of the community (Wiig, 2018). This case and further examples from the literature demonstrate how surveillance, though not without its flaws, can help to improve neighbourhoods and bring direct benefits for citizens (Klauser, 2007; Wheeler, 2016; Wiig, 2018).

In addition, while the actual effectiveness of surveillance technologies in terms of crime reduction is heavily debated (see Section 2.2.4.), the effect on fear of crime is far less controversial. Several authors find that citizens feel safer and more confident when SOSTs are visibly in operation (Heger, 2010; Rothmann, 2010; Zurawski & Czerwinski, 2007). This supports the hypothesis, that individuals who are afraid of being victimised or whose life is significantly impacted by crime are more likely to see the installation of a new SOST as beneficial and thus acceptable.

6.2.3. Contact with the Police and Trust in Police

Several studies link a higher trust in police with an increased willingness to accept new surveillance measures and SOSTs (Davis & Silver, 2004; Kochel, 2018; Trüdinger & Steckermeier, 2017). Research further shows that the general attitude individuals have towards the police and authority in general is an important predictor for support for police action and new tactics and techniques (Tyler and Huo 2002; Sunshine and Tyler 2003; Jackson et al. 2013; Yesberg and Bradford 2019; Bradford et al. 2020). Other researchers such as Milani (2020) find that police decisions and activities are deemed to be acceptable just as long as these actions are considered within certain normative bounds. Within these bounds, however, almost any action is seen as justifiable. As such, trust in the police and can be considered an essential factor in predicting individuals' attitude towards new SOSTs (Thompson et al., 2020; Trüdinger & Steckermeier, 2017). The greater the trust in them, the less threatening the video surveillance should appear. As such, the following hypothesis will be explored:

H_4 High trust in the police positively influences the social acceptability of new SOSTs.

Closely connected to this is the issue of previous experiences with the police and their impact on the acceptance of new SOSTs (Reisig & Parks, 2000; Rothmann, 2010). As discussed in the academic literature about various other policing tools and techniques from the use of tasers to community policing or racial profiling (Bradford et al., 2020; Yesberg et al., 2020), it is not a far-fetched hypothesise that previous negative experiences with the police can positively or negatively impact how an individual might view increased powers for authorities and the use of new technologies. This study considers prior contact with the police as a possible pre-treatment effect, asking respondents to elaborate whether they had previous encounters with the police and whether these had been positive, negative, or mixed. This in turn helps to explore the following hypothesis:

H_5 Individuals who have previously had some or exclusively negative encounters with the police are less likely to accept the deployment of new SOSTs.

6.2.4. Mediating Effect of Trust in Police

Previous positive or negative encounters with the police do, however, not only impact the level of social acceptability directly. Instead, they are also an important factor in predicting how individuals see the police and thus by proxy how their behaviour towards additional powers or the deployment of new SOSTs may be shaped (Cheurprakobkit, 2000; Dai, Hu, & Time, 2019; Zevitz & Rettammel, 1990). Van Damme (2017) explored the impact of positive and negative interactions with the police and the impact on trust in the police. The study finds that unsatisfactory contact was associated with lower trust and more positive encounters with higher trust and that positive encounters had a stronger (positive) impact than the detrimental effect of negative encounters (Van Damme, 2017). As such, trust in police can act as a mediating variable between previous experience with the police and the level of social acceptability of a new SOST. While the literature distinguishes between police-initiated and citizen-initiated contact (Li, Ren, & Luo, 2016). Police initiated encounters (e.g., arrests or traffic stops) are more likely to be negative and thus for obvious reasons more likely to lower satisfaction and public attitudes of police (Li et al., 2016; Schafer, Huebner, & Bynum, 2003; Skogan, 2005; Weitzer & Tuch, 2005). Here, procedural justice is important as unfair or unjust treatment (or even the perception of such) can have severe negative effects on individuals' attitude towards the police (Wells, 2007). Overall, this means that previous experiences with the police can predict both individual attitudes towards new SOSTs directly and by proxy through the variable of trust. In case of the latter, trust in police mediates the impact of previous experiences with the police on the level of social acceptability (see the conceptual map in Figure 6). Thus, the following sub-hypothesis can be formed.

H_{5A} Individuals who have previously had some or exclusively negative encounters with the police are less likely to trust the police.

Furthermore, as trust in police is a complex concept in itself and impacted by a variety of factors, it may function as a mediating variable for several of the other hypothesised predictors. This includes in addition to previous encounters with the police also victimisation experience, the impact of crime, and the individual political attitude.

With regards to victimisation experience and the impact on crime on the individual, research shows that attitudes towards the police and thus also towards new SOSTs are shaped by crime and safety in individuals' neighbourhood (Dai, Hu, & Gu, 2020; Dai & Johnson, 2009; Reisig & Parks, 2000; Weitzer & Tuch, 2005). Citizens' perception of local crime problems and the impact of crime (and fear of crime) on their life significantly predicts their perception of and attitude towards the police (Dai & Jiang, 2016). The direction of this impact is, however, topic of controversy. Some authors suggest that citizens that live in high-crime neighbourhoods tend to be less satisfied with the police and have a lower expectation of police effectiveness due to their own experience (Dai & Jiang, 2016). This is supported by studies that find that there tends to be a higher rate of police misconduct in these neighbourhoods (Kane, 2002) leading to more direct negative experiences with the police and increased mistrust (Schafer et al., 2003). The before-mentioned study by Kochel (2018) suggests that especially individuals living in high-crime neighbourhoods that need police intervention are likely to accept police intervention and increased use of SOSTs. While these points seem to be contradictory at first, this research suggests that individuals living in high crime neighbourhoods, i.e., those affected by crime and fear of crime and with a high risk of victimisation, are more likely to accept SOSTs as they are interested in solutions to their situation. At the same time, they might have lower trust in police as police due to a strained relationship, negative experiences, or a lack of trust in the ability of the police to tackle crime effectively. As such, the following two sub-hypotheses can be formulated:

H_{5B} *Individuals who have previously been victimised are less likely to trust the police.*

H_{5C} *Individuals whose life is heavily impacted by crime and the fear of crime are less likely to trust the police.*

As discussed before, personal political beliefs strongly impact how individuals feel about the police and authority in general. This is further explored by Anania et al. (2019) who finds that individuals with more conservative attitudes have more trust in police and the ability of police to provide safety and security than those with more liberal mindsets. As a result, the following sub-hypothesis can be formulated:

H_{5D} *Individuals with more left-wing political opinions are less likely to trust the police.*

6.2.5. Privacy Concerns

The last important factor to discuss are privacy concerns and their impact on the social acceptability of new SOSTs. More broadly, this includes general personal attitudes towards privacy and the use of personal data by the government (Nguyen et al., 2011).

Unlike the previous factors, privacy concerns require a more thorough introduction as defining the 'evanescent concept' of privacy is not an easy task (Gormley, 1992; Smith, Dinev, & Xu, 2011). These definitional issues arise from the context-bound nature of the concept of privacy (Thierer, 2013; Whitman, 2003). In addition, 'privacy' does not describe a single phenomenon but can be broken down in a number of different categories including information privacy, territorial privacy, bodily privacy, and privacy of communications (Banisar & Davies, 1999).

Definitions of privacy vary in scope and focus throughout the literature but often involve two dimensions, privacy as a right and privacy as a commodity (Smith et al., 2011). Early conceptualisations of privacy often define it in a normative manner as a 'right to be left alone' (Brandeis & Warren, 1890). With the beginning of the 20th century and with ever increasing speed in the 21st century, the focus has shifted more and more towards a reconceptualisation around the value of privacy as a commodity and its exchange for benefits of security and economy (Campbell & Carlson, 2002).

Many of the well-established concepts in the realm of privacy research begin to crumble as new technologies reshape societies and interactions between governments and citizens. One example of this is the fact that traditionally the private sector was thought of as a threat to information privacy, a fact that has increasingly changed with the gathering of massive amounts of data for example on online behaviour by governments (Wilton, 2017).

As with so many scientific concepts, there is no unified single definition of privacy as such. Nevertheless, there are useful approaches to make 'privacy' a useful and practical concept. One of these approaches is understanding privacy in terms of control. One famous example of this is the definition of Westin (1967) who describes privacy as 'the right of the individual to decide what information about himself should be communicated to others and under what condition.'

Control is also discussed in more recent literature (Nam, 2017). Several definitions of control, or privacy control, refer to it as the (perceived) extent to which individuals can influence their environment or the collection and usage of their data (Brandimarte, Acquisti, & Loewenstein, 2013; van Heek et al., 2017). In practice, the literature finds a paradox and somewhat counterintuitive relationship between individuals' privacy concerns and their actual personal information disclosure behaviours (Awad & Krishnan, 2006; Dienlin & Trepte, 2015; Norberg, Horne, & Horne, 2007). Today, many privacy scholars advocate for contextual approaches to information privacy (Wu, Vitak, & Zimmer, 2020).

The research suggests that even though many people may hold privacy concerns, those who make concerted efforts and take action to control their data are also more concerned about increased data gathering by external entities such as the government (Nam, 2017). Some of the most important factors influencing the acceptability of new SOSTs and surveillance in general are privacy concerns (Dinev et al., 2006; Dinev et al., 2008; Smith et al., 2011) and the perceived need for a new intervention or new surveillance powers (Brown & Korff, 2009; Dutton, Guerra, Zizzo, & Peltu, 2005). Surveillance concerns are information privacy concerns in the context of government surveillance or as Dinev et al. (2008: 220) describes it, 'a negative belief about the proactive gathering and processing of personal information and monitoring [of] online behaviour by the government'.

The increasingly normalised usage of more and more intrusive SOSTs creates a state of permanent surveillance, which many authors argue significantly infringes on individual's privacy (Cannataci, 2010; Levi & Wall, 2004; Lodge, 2007a; Patton, 2000; Webb, 2007). While citizens are generally willing to sacrifice some privacy for the sake of (at least the feeling of) security, privacy concerns are often highly nuanced and can have a devastating impact on any SOSTs (Davis & Silver, 2004). Privacy concerns are highly important for the functioning of SOSTs as they can influence the effectiveness of camera operations (Cerezo, 2013). La Vigne et al. (2011b) for example describe how political pressure by citizens effectively limited the monitoring abilities of CCTV, emphasising that it is crucial for police or government to build public support for SOSTs.

Nam (2018) discusses the complex relationship between privacy concerns of individuals and the social acceptability of surveillance technologies. The study finds that especially perception of public benefits from government surveillance and political attitude serve as key predictors for the acceptance of surveillance technologies (Nam, 2018). In addition, control over how data were gathered and used affected privacy concerns more than the acceptability of new interventions (Nam, 2018).

Concerns about the handling of personal data by the government and diminishing trust in the government's ability to keep data safe are also enhanced by a number of high-profile cases. These include the unwarranted wiretapping of phones (Baldwin Jr & Shaw, 2006), indiscriminate mass surveillance (Wilton, 2017), or instances of hacking and data breaches (Furnell, Heyburn, Whitehead, & Shah, 2020; Oxford Analytica). In this study, privacy concerns in general and those specifically pertaining to the gathering and use of data by the government will be used as predicting variables. Privacy concerns are highly complex (Nam, 2017). They can be rational or irrational in any given situation and may be based on cost-benefit calculations, heuristics, emotions, or (mis) perceptions of a situation (Acquisti, Brandimarte, & Loewenstein, 2015; Awad & Krishnan, 2006; Brandimarte et al., 2013; Braun et al., 2018; Culnan & Armstrong, 1999; Culnan & Bies, 2003; Etzioni, 2005; Klopfer & Rubenstein, 1977; Laufer & Wolfe, 1977; Li, 2012).

Questions surrounding the issue of privacy concern were created on the basis of the Concern for Information Privacy Model (CFIP) which outlines four broad areas that drive the concern for information privacy of the individual. These areas of concern include the collection of personal data, the risk of improper access, the potential for unauthorised secondary use, and the challenge of preventing or correcting errors in the data (Nguyen et al., 2011).

Given that government surveillance involves the collection and use of personal information and data about citizens and given that it occurs primarily in an already secretive security context, it might be expected that individuals who are concerned about the collection or use of their personal information are less likely to find new SOSTs acceptable (Hallinan & Friedewald, 2012; Thompson et al., 2020). Thus, this study hypothesises:

H_6 General privacy concerns negatively influence the acceptability of new SOSTs.

H_7 Privacy concerns about how the government collects and uses personal data negatively influence the acceptability of new SOSTs.

6.2.6. Mediating Effect of Privacy Concerns

Similar to trust in police, privacy concerns are likely to impact the level of social acceptability directly but might also mediate effects of other variables. One of the core foundations for privacy concerns are the personal beliefs and political ideology an individual subscribes to[18] (Best & Krueger, 2011; Krueger, 2005). The literature suggests that those with liberal or left-wing beliefs are more likely to voice privacy concerns (Anania et al., 2019; Omrani & Soulié, 2020). Thus, this thesis hypothesises that the privacy concerns, both general and pertaining to the government, mediate the effect of political affiliation on the acceptability of new SOSTs.

H_{7A} Individuals with more left-wing political opinions are more likely to have general privacy concerns.

H_{7B} Individuals with more left-wing political opinions are more likely to have privacy concerns about how the government collects and uses personal data.

6.2.7. Demographic factors – Age, Gender, Ethnicity

Throughout the academic literature, demographic factors are often included as important predictors of social acceptability when discussing interaction with the police or the introduction of new security measures. Also in terms of surveillance, issues of gender, ethnicity, and age play a role and are often considered to be important shapers of attitudes towards the government (Krueger, 2005; Nam, 2018; Reddick et al., 2015; van Heek et al., 2017; Zurawski & Czerwinski, 2007). Overall, much of the academic literature agrees that demographic factors such as age and ethnicity, or political affiliation and other personal beliefs and experiences can predict how individuals view new surveillance interventions (Hallinan &

[18] The literature in some instances suggests a reciprocal relationship between personal political beliefs and concerns about government surveillance.

Friedewald, 2012). Age, gender, ethnicity and nationality are only some of the demographic variables that the literature identifies (Hallinan & Friedewald, 2012). Both age and gender are often discussed in terms of vulnerability and fear of crime (Li, 2018; Pryce et al., 2018). Several studies discuss the relevance of gender for the attitude towards surveillance measures and as predictors of relations with the police (Reuband, 2001; Reuter et al., 2016; Rothmann, 2010; Töpfer, 2004; Zurawski & Czerwinski, 2007).

Because of their overarching nature, however, both variables will be included in the analysis as variables to control for any impact they might have on other latent constructs but no concrete hypotheses about their impact will be formulated, and they will not be discussed at length in this chapter.

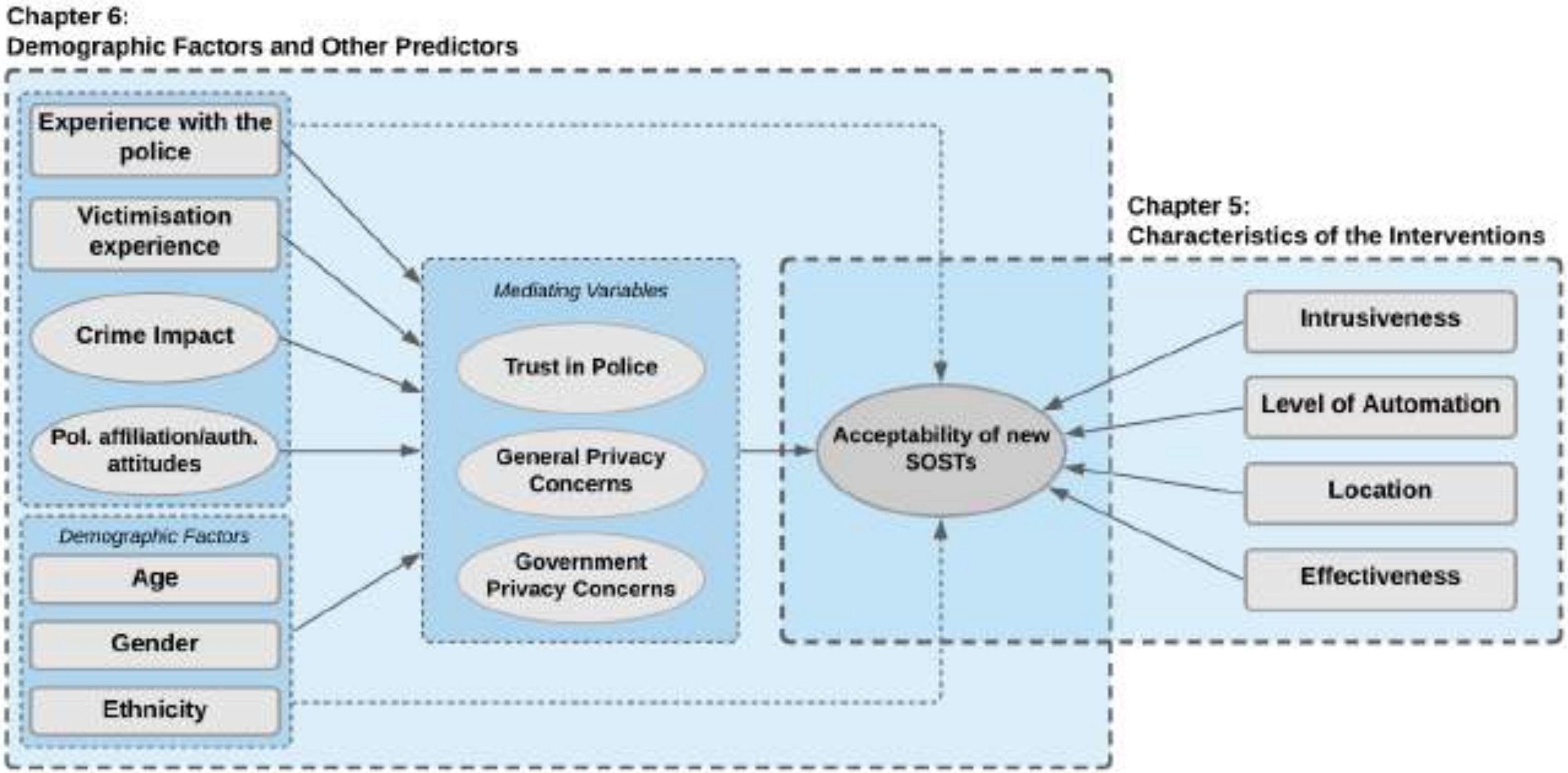
Ethnicity will be treated in the same fashion, as it has been awarded much importance in the academic debate with a substantial body of literature attributed to it and its predictive power for people's perception of police and as a determinant of trust (Italiano, Ramirez, & Chattopadhyay, 2021; Skoy, 2021). Especially more recently, the debate has gained traction with the tragic case of George Floyd and Black Lives Matter protests around the world (Italiano et al., 2021; Yesberg et al., 2020). In the UK, the so-called 'racial perception gap' and overall lower satisfaction and confidence in the police in a majority of black communities (Phillips & Bowling, 2020), may heavily impact how individuals view increased surveillance capabilities and more intrusive tools for the police. The literature also suggests that there is a correlation between ethnic group and previous experiences with the police often pointing towards discriminatory practices such as racial profiling (Durlauf & Heckman, 2020; Keenan, 2021).

Even though ethnicity as a factor in police-community relations is today hotly debated, it is not uncontroversial as in the context of measuring public acceptability. Authors such as Ellison (2005) discuss for example whether it is necessary to use ethnicity or colour of skin as measures at all, arguing that in many instances they is used as a proxy for other factors. In this case, the literature suggests that ethnic minorities have generally a worse relationship with and less trust in the police and as such would be less inclined to support a more intrusive crime detection technology.

Another problem with using ethnicity as a measure is of practical nature and occurs in the data collection and presentation stages. It is often not practical or viable in terms of resources, to compare small groups as it would mean group comparisons would need significant amounts of additional respondents to satisfy requirements in terms of sample size for each group. Thus, research that is not primarily focussed on comparing groups based on ethnicity often tends to group individuals in broader categories which may not overlap in terms of experiences, heritage, or cultural affiliation (e.g., grouping individuals from Indonesia and Mongolia together in an 'Asian' category may not be the most useful approach).

Despite these issues, a majority of studies suggest that including ethnicity or visual features such as skin tone can be useful. For example, a growing body of literature demonstrates that facial recognition algorithms and AI may have inbuilt (racial) biases (Ferguson, 2019; Garvie & Frankle, 2016; Lee et al., 2017; Lee, 2018; Noor, 2020). Here, ethnicity/the colour of individuals' skin is the only relevant factor, as the image detection algorithms only discriminate based on it. This means that despite the criticism, that ethnicity or in this case skin colour can be an important factor when discussing surveillance. As such, ethnicity is similar to age and gender included as a control variable.

Figure 6 Conceptual map of variables and analysis approaches



6.3. Method

The following method serves to analyse the data of the same vignette study discussed in the previous chapter and builds in parts on the findings discussed there. This means, as mentioned before, that this chapter moves from an experimental to a correlational paradigm. While this study still takes into account that individuals were assigned different conditions, these were controlled for in the analysis. While the effects of the experimental variables on the outcome variable (level of acceptability) were still given, the randomisation of respondents means that these effects should not impact the results of this study. To ensure only the acceptability of new SOSTs was considered, observations from the groups that included only traditional CCTV systems were dropped from this analysis. An in-depth discussion of the experimental study design can be found in Section 5.3. A summary of all variables and the conceptual underpinnings can be found in Figure 1 above.

6.3.1. Structural Equation Modelling as a Method

Structural Equation Modelling (SEM) was chosen to explore the complex net of relationships between the independent variables as well as their impact on social acceptability. The method refers to a statistical procedure to test or find correlative relationships between multiple variables.

SEMs are widely used and increasingly popular in social sciences as they are well suited for such a task (MacCallum & Austin, 2000; Saris, Satorra, & Van der Veld, 2009). A special feature of SEM is that it allows for the inclusion of latent, i.e., not directly observable, variables (Krempel, 2016). A good example of a latent variable or construct is the intelligence of a person. It cannot be measured directly, but must be measured indirectly via several sub-questions, the so-called items. Different items cover the different aspects of intelligence, such as linguistic, computational, and spatial thinking.

The model presented in this thesis also examines a number of latent constructs, namely the acceptability of the intervention, the impact of crime and fear of crime on individuals, the political orientation and authoritarian attitudes, trust in police, general privacy concerns, and privacy concerns about the use of data by the government. As with the above-mentioned example of intelligence, the individual items used to measure each of these variables aimed to capture a different aspect of the construct. For example, items for the construct of impact of crime and fear of crime measured the impact of crime in the area of residence, the impact on crime on one's life, and the impact of fear of crime (see Table 24). In addition to these constructed variables, the study also included directly measured variables, namely victimisation experience and previous experiences with the police, as well as the demographic factors of age, gender, and ethnicity.

The SEM can be used for both exploratory and confirmatory purposes (Krempel, 2016). In this work, it is used as the latter to confirm relationships that can be reasonably hypothesised, based on the existing literature.

For this purpose, the SEM distinguishes between the measurement and the structural model (Krempel, 2016). The measurement model summarises the constructs and the related items, whereas the structural model describes the hypothesised relationships between the different latent constructs. Figure 7 depicts the relationships within the SEM and the general structure. Firstly, the measurement model and a confirmatory factor analysis (CFA) were conducted, which served to confirm the indicators and factors in the model and to assess whether the constructed composite variables are valid and reliable before testing the hypotheses (Bomfim, de Souza, & Corrente, 2018). In a second step, the structural relationships between the variables were explored using the structural model.

6.3.2. Confirmatory Factor Analysis (CFA)

The goodness of fit of the model was assessed by interpreting the Chi^2-statistic, the standardised root mean squares residual (SRMR), the root means square error of approximation (RMSEA), the Tucker-Lewis Index (TLI), and the comparative fit index (CFI) following Aichholzer (2017). Table 23 below provides the cut-off values that were used to determine the fit of the model. For a more detailed explanation of fit indices and an in-depth discussion of their calculation see West, Taylor, and Wu (2012).

Table 23: Goodness of fit measures and cut-off values based on West et al. (2012)

Fit index	**Cut-off criterion**	**Theoretical range**	**Reference**
Chi^2 [a]	$p < 0.05$	> 0	Jöreskog (1969)
SRMR [a]	< 0.08	> 0	Bentler (1995)
RMSEA [a]	< 0.06	0-1	Rigdon (1996)
TLI	> 0.95	0-1 [b, c]	Tucker and Lewis (1973)
CFI	> 0.95	0-1	Bentler (1990)

[a] Fit index is sensitive to N.

[b] Can be negative. Negative values indicate an extremely ill specified model.

[c] Can be >1, indicating an extremely well-fitting model.

Table 25 shows the goodness of fit values of the CFA model, which are significant with Chi^2(470) = 1735.986 ($p < 0.001$), CFI=.957, TLI=.952, SRMR=.049 and RMSEA=.043. While there are several rules of thumb and cut-off values floating around, all following different arguments about how the reliability of scales could be increased by deleting items, this study retains all items. This is done on the basis that the scales employed in this study are proven from the literature and even with low factor loadings, individual items contribute conceptually to the overall latent construct.

Table 24: Results of the Confirmatory Factor Analysis

Constructs and their items	**Std. Loading**	**R^2**
Acceptability		
How acceptable do you find the installation of the new system?	.974***[1]	.949
Do you support or oppose the installation of the new system?	.976***	.952
How concerned would you be about the installation of the new system?	.871***	.758
Do you think the system will be good or bad for the neighbourhood?	.809***	.652
Crime Impact		
How much of a problem is crime in the area where you live?	.531 ***[1]	.634
How much is your own quality of life affected by crime?	.771***	.230
How much is your own quality of life affected by the fear of crime?	.716***	.508
Political Belief		
Where do you see yourself on the political spectrum?	.937***	.878
Do you think that people who break the law should be given stiffer sentences?	.810***	.657
Should schools teach children to obey authority?	.885***	.785
Trust in Police		
When police deal with people they almost always behave according to the law. [a]	.768***[1]	.186
When police deal with people, they almost always respect people's rights. [a, b]	.798 ***	.568
When police deal with people, they often arrest people for no good reason.	.692***	.618
Police officers make decisions based on facts.	.780***	.459
Police officers explain their decisions to the people with whom they deal.	.767***	.590
Police officers treat people with respect. [b]	.848***	.566
The police provide the same quality of service to all citizens. [c]	.775***	.705
The police treat everyone fairly, regardless of who they are. [c]	.775***	.233
Police effectively tackle gang activity and related crimes. [d, e]	.443***	.581
Police effectively respond to emergencies promptly. [d]	.493***	.581
Police effectively deter crimes when patrolling. [d, e]	.407***	.476
I am comfortable allowing the police to decide how to best deal with crime and disorder. [f]	.698***	.340
If I were a victim of crime, I would be happy to let the police deal with this matter. [f]	.590***	.437
I am happy to accept the ability of the police to intervene in people's lives. [f]	.671***	.159
General Privacy Concern		
It is the most important thing for me to protect my privacy. [g]	.400*** [1]	.159
I am comfortable telling other people, including strangers, personal information about myself.	.765***	.587
I try to minimise the number of times I have to provide personal information about myself. [g]	.511***	.262

I am comfortable sharing information about myself with other people unless they give me a reason not to.	.801***	.640
I have nothing to hide, so I am comfortable with people knowing personal information about me.	.683***	.468
Government Privacy Concern (Thinking about how the government collects and uses your personal data…)		
People have lost all control over how personal information is collected and used.	.615*** [1]	.381
Personal information is always handled in a proper and confidential way.	.786 ***	.619
Existing laws and practices provide enough protection for peoples' privacy.	.755***	.566
Peoples' best interests are not always kept in mind when handling their personal information.	.533***	.285

Note: *** Significant at p<0.001, [1] Loading fixed to set the scale, $^{a\text{-}g}$ denominate correlated error terms

Table 25: Goodness of Fit Measures of the CFA

Measures	Model
Chi^2	1735.986 (p< 0.001)
SRMR	0.049
RMSEA	0.043
TLI	0.952
CFI	0.957

6.3.3. Structural Equation Model

To examine the effect of personal attitudes and beliefs, as well as demographic factors on the level of social acceptability, a Structural Equation Model (SEM) was specified. The model tested the before-mentioned direct, i.e., the impact of the variable on the outcome, and indirect, i.e., mediated, effects. This included the effects of victimisation, previous experiences with the police, crime impact, political affiliation, trust in police, general privacy concerns, as well as privacy concerns with regards to the government. In addition, all latent variables in the model were regressed on the control variables age, gender, ethnicity. An in-depth discussion of the latter can be found in the previous chapter.

As previously mentioned, connections and correlations in the SEM were based on the academic literature and previous studies. In cases where no previous studies could be found, plausible associations were drawn based on thematic commonalities and similarities in the question design (Bomfim et al., 2018). A structural equation model was formulated to test the proposed relationships using a maximum likelihood estimator (Aichholzer, 2017).

Once again, goodness of fit indices were used to assess the model fit to the data (Table 26). The indices showed that the initial model, which had been based on the conceptual framework, did not have a good fit with the data. After several improvements were made, using modification indices, and exploring possible correlations between variables, the final model was created. As many of the questions within the distinct constructs were phrased similarly, reverse worded, or were thematically to some extent overlapping, correlations between error terms were allowed, following the suggestion by Brown (2015, p. 157). The then calculated goodness of fit indices suggested that the observed data was much better represented by this model. With the exception of the Chi^2-Test, which is highly sensitive to sample size, all fit indices indicated a good fit of the model.

Table 26: Goodness of fit measures of the final model

Measures	**Model**
Chi^2	2238.200 (p< 0.001)
SRMR	0.058
RMSEA	0.041
TLI	0.943
CFI	0.948

To estimate the direction of the association between the variables, the standardised coefficients (SC) were interpreted. For this, Kline suggest that an SC of 0.10 indicates a small effect, 0.30 > SC > 0.10 indicates an average effect, and SC > 0.50 indicates a strong effect.

The model included a number of latent constructs that were each measured through several items, some directly measured variables were also included. These included victimisation experience, experience with the police, and the control variables age, gender, and ethnicity. While victimisation was a dichotomous variable (i.e., coded as either yes or no), a reference group had to be specified for the other variables against which all other possible conditions of that variable were compared (Aichholzer, 2017). For experience with the police, 'no experience' was chosen as the reference group. For age, the group 65+ was used as a reference group. In the control variable 'gender', 'female' was used as the reference, meaning that the results are to be interpreted as a comparison to this. Lastly, in the ethnicity variable, 'white British' was used as the reference group.

6.4. Results of the SEM

Table 27 and Figure 7 show the results of the SEM. The coefficients in Figure 7 give an indication of the strength of the relationship between the variables as well as their indicators. It can be observed that many of the examined variables have a significant effect on the acceptability of the intervention. The before-mentioned coefficients, do, however, only shine light on the direct effect. In some cases, the direct effect between a variable and the level of social acceptability was mediated by other variables (Faller & Scheiner, 2020). Trust in police as well as the two privacy concern variables served as mediating variables, with acceptability in all analyses as the outcome variable. The total influence of a variable on the social acceptability ultimately calculated from the sum of the direct and all indirect effects. Indirect effects are calculated as the product of all path coefficients leading to the outcome variable. For example, the overall effect of the crime impact in the overall model is calculated as .097+(-.074)*.25=0.078. Table 27 presents the coefficients of the direct, indirect, and total effects for all examined variables. In some cases, the effects are amplified in others weakened by the mediating variable.

Table 27: Standardised direct, indirect, and total effects on social acceptability

Variable	Effect on the level of social acceptability		
	Direct effect	**Indirect effect**	**Total effect**
Latent Constructs			
Crime Impact	.0970384***	-.0183935*	.0786449**
Political belief	.183538***	.0989383***	.2824763***
Victimisation	-.0150495	.0077041	-.0073454
Neg. exp. with police	-.0074216	-.0445315***	-.0519531*
Mixed. exp. with police	-.0941651	-.0366159***	-.130781**
Pos. exp. with police	-.0541412	.0462665***	-.0078747
Control variables (regressed on all other variables)			
Age			
18-24	-.0535156	-.1044965***	-.1580121***
25-34	-.1088448***	-.0998735***	-.2087183***
35-44	-.0937875**	-.0674258***	-.1612133***
45-54	-.0675511*	-.026251	-.0938021**
55-64	-.0513117	-.0368986*	-.0882103*
Gender			
Male	-.0566201*	.013275	-.0433451*
Other	-.0195344	-.0306066*	-.050141*
Ethnicity			
Mixed	-.0093128	-.0298448	-.0391576
Asian	.0305983	-.0270911*	.0035072
Black	.0205305	-.0406644*	-.0201339
Other	.0168023	-.0148933**	.001909
Mediating variables			
Trust in police	.2472266***	N/A	.2472266***
Privacy general	-.0767859**	N/A	-.0767859**
Privacy government	-.1618101***	N/A	-.1618101***

*= p<0.05, **= p<0.01, ***= p<0.001

Table 28: Variance explained by the endogenous latent variables

Variable	R^2
Trust in police	.21939
Privacy general	.0042429

Privacy government	.0326164

In addition to the experimental conditions discussed in Chapter 5[19], several other possible predictors of the acceptability of new SOSTs were tested here. These included trust in police, previous victimisation, political affiliation, the impact of crime and fear of crime, previous experiences with the police, and both general and government-specific privacy concerns. The results of the analysis also give insights into which demographic and pre-treatment factors predicted the level of social acceptability of the new intervention best. Overall, almost all tested factors had a significant impact on the level of social acceptability. In the following, the

6.4.1. Political Beliefs

The political beliefs of the participants also showed to be a significant factor in predicting the social acceptability of the new technology, as both direct (β=.184 *t*=7.45, *p*<.001) and total (β=.283 *t*=11.36, *p*<.001) effects could be found. Unsurprisingly, the results suggest that individuals leaning towards the right of the political spectrum and those with stronger authoritarian attitudes also find more intrusive interventions more socially acceptable than individuals on the political left. These findings support Hypothesis 1.

The results also suggest a mediating effects of trust in police and privacy concerns were present. Individuals on the political right demonstrated significantly greater

[19] The experimental conditions were also tested in the SEM before dropping traditional CCTV observations. The level of automation was found to be negative and significant (β=-.127, t=-5.04, p<.001) similar to the intrusiveness of the system (β=-.328, t=-16.03, p<.001). Neither the level of effectiveness (β=.005, t=.92, p>.1), nor the change location had a significant effect (β=.02, t=.92, p>.1). This echoes the findings of Chapter 5.

trust in the police (β=.302 *t*=9.85, *p*<.001) than those on the political left, which supports Hypothesis 5D.

Interestingly, a more conservative political belief was associated with lower privacy concerns about the use of data by the government (β=-.181 *t*=-5.84, *p*<.001) but slightly greater general privacy concerns (β=.065 *t*=2.15, *p*=0.032), once again highlighting the strong connection between personal political beliefs and trust in police and government. While these findings support Hypothesis 7B, they contradict Hypothesis 7A.

6.4.2. Victimisation Experience

Surprisingly, victimisation experience was not a significant predictor of any other variable. This goes both for direct and indirect effects on the level of social acceptability as well as trust in police. Thus, neither Hypothesis 3, nor Hypothesis 5B could be confirmed.

6.4.3. Crime Impact

The impact of crime and fear of crime on people's lives showed to be a significant predictor of social acceptability, as significant total effects could be observed (β=.078, *t*=2.89, *p*=0.004). In addition, trust in police had a mediating effect on crime impact, and individuals who were more impacted by crime or fear of crime had lower trust in the police (β=-.074, *t*=-2.72, *p*=0.006). These findings support both Hypothesis 2 and Hypothesis 5C.

6.4.4. Experiences with the Police

Previous experiences with the police both positive and partly or entirely negative were mediated by trust in police. While only positive experiences with the police were associated with increased trust in police (β=.187, *t*=5.98, *p*<.001), both mixed (β=-.148, *t*=-4.73, *p*<.001) and entirely negative (β=-.180, *t*=-6.49, *p*<.001) experiences with the police resulted in lower trust. Thus, trust in police mediated the effect of experience with the police on the level of social acceptability. These findings support Hypothesis 5A.

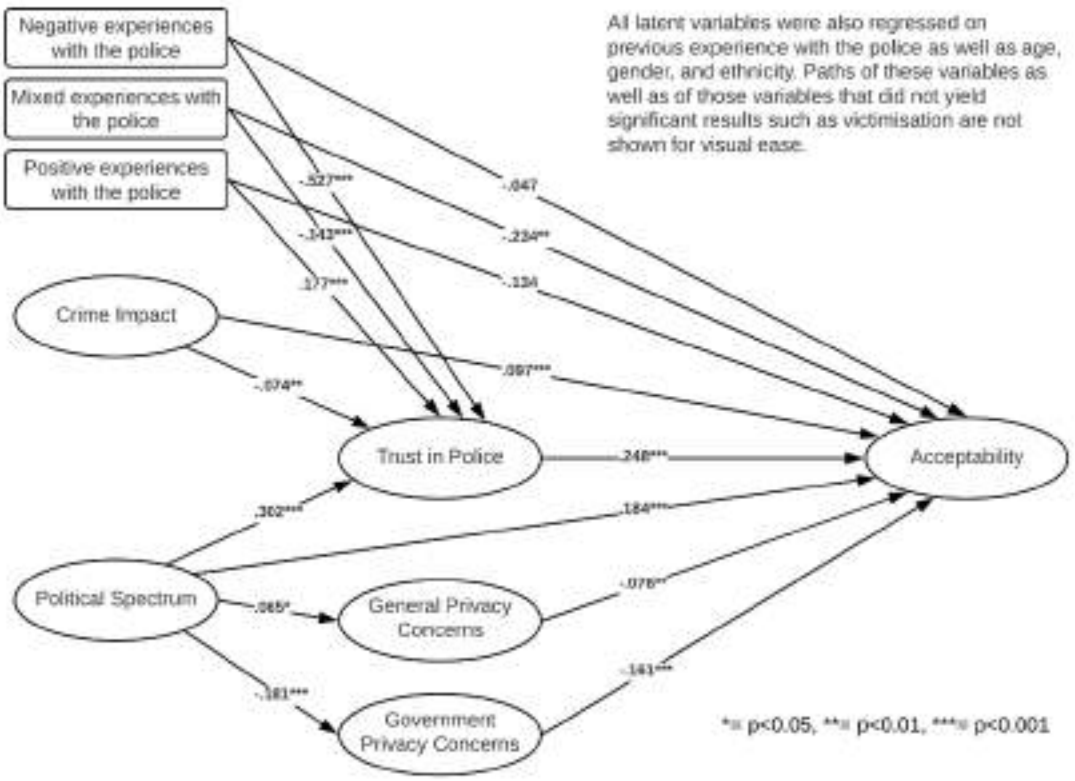
Despite this, however, only mixed (β=-.129, *t*=-4.33, *p*<.001) and negative experiences (β=-.051, *t*=-2.14, *p*=0.032) had a total effect on the level of social acceptability. This means that individuals who have made some or exclusively negative experiences with the police found the deployment of new SOSTs less acceptable, ultimately supporting Hypothesis 5.

6.4.5. Trust in Police

The relationship individuals had with the police played a significant role in predicting their acceptance of the new surveillance system. The analysis found that individuals with high trust in police (β=.248, *t*=7.34, *p*<.001) were likely to show a higher acceptability towards the deployment of new SOSTs. In addition, trust in police mediated a number of other variables, as discussed before. The findings support Hypothesis 4.

6.4.6. Privacy Concerns

Both, individuals with existing general privacy concerns (β=-.076, *t*=-2.80, *p*=0.005) and those particularly concerned about the use of personal information by the government (β=-.161, *t*=-4.92, *p*<.001) were less trusting of the new surveillance technologies and overall, significantly more critical. These findings support Hypotheses 6 and 7.



All latent variables were also regressed on previous experience with the police as well as age, gender, and ethnicity. Paths of these variables as well as of those variables that did not yield significant results such as victimisation are not shown for visual ease.

Figure 7 Structural model with acceptability as the ultimate response variable

6.5. Discussion

The following discussion with closer examine the results of the analysis and contextualise them in the academic debate.

6.5.1. Political Beliefs

The political spectrum had both, significant direct and indirect effects on the social acceptability of the intervention. A strong total effect could be observed indicating that individuals on the political right were more accepting of the intervention than those on the political left. This contradicts the findings by Lauber and Mühler (2017) who do not identify a correlation between political attitudes and the confidence and trust in the police. Instead, they suggest that the noticeable high level of trust in the police is not the result of widespread conservative attitudes (Lauber & Mühler, 2017). Their research, however, provides the caveat that the findings are only to be understood as an indication at first. While they rule out that primarily political stereotypes are underlying predictors of trust, they find that content or quality of police work inevitably form the basis of trust (Lauber & Mühler, 2017). Therefore, on the one hand, it should be examined more closely which aspects of police work particularly promote trust and, on the other hand, consideration should be given to which other factors also play a role in building trust.

6.5.2. Crime Impact

The analysis found that individuals whose life is impacted by crime or fear of crime to a significant level, are more likely to accept new crime prevention interventions. At the same time, individual experiences of victimisation did not prove to be significant for the evaluation of video surveillance. This means that people who have been victims of crime rate the use of surveillance no differently than people who have not reported being victims of crime if socio-demographic variables are also considered. Overall, these results echo much of the academic literature in suggesting that fear of crime and the impact of crime on the daily life of individuals is a significant predictor of social acceptability of new SOSTs.

Crime impact further had a significant negative impact on trust in police, indicating that those impacted by crime in their daily lives had lower trust in police. This means that though individuals affected by crime and fear of crime found the deployment of SOSTs more acceptable than those less affected, they also showed less trust in police. At a first glance, these findings seem to be contradictory. It may, however, be the case that people living in precarious neighbourhoods or generally afraid of crime consider SOSTs a practical solution to their problems. They might have negative associations with the police as they consider them to be unable to tackle crime as is.

The question of whether SOSTs can contribute to a feeling of safety is, however, controversial. Even though an overwhelming majority of studies find a positive effect of CCTV and other surveillance technologies on crime and fear of crime (Ceccato, 2020a), these findings are contingent on the specifications of the surveillance intervention. Feelings of safety depend to a large extent on the visibility of measures. Increased lighting for example often increases the feeling of safety because it has a highly visible impact on the environment (Ceccato, 2020b; Kyba, Kuester, & Kuechly, 2017; Struyf, 2020). Thus, the visibility of the intervention and of its impact are crucial to improve the feeling of safety for citizens. As respondents were given clear information about the intervention, the impact of the proposed system was clear to them, which could explain the increased level of acceptability from those impacted by crime and fear of crime.

The findings further emphasise the importance of personal experiences with crime and police as a decisive factor for social acceptability of new SOSTs. Ultimately, this study confirms several findings from the literature, first and foremost that while for some people the presence of SOSTs can create stress and fear of observation, it makes others feel empowered and safe (Koskela, 2002; Yavuz & Welch, 2010).

6.5.3. Experience with the Police and Trust in Police

The effect of experiences with the police was mediated by trust in police. This means that individuals who previously had made negative experiences trusted the police less and as a result also found the deployment of new SOSTs less acceptable. Trust in police in turn was a significant predictor of the social acceptability of the interventions. Unsurprising, individuals who trusted the police more were also more accepting of new SOSTs. Both of these findings are crucial to the overall discussion and have implications for the deployment and use of new SOSTs, especially in a policing context.

Firstly, these findings indicate that negative experiences with the police can not only be detrimental to trust in police as such but can also negatively impact the acceptance of new SOSTs. As such, regular police interactions, that on the surface have nothing to do with SOSTs, can either lay the foundation for support of new technologies or diminish their acceptance in the population. This is supported by various studies highlighting the importance of pre-existing favourable attitudes towards the police and trust in the police when predicting the acceptability of new police powers or measures (Kyprianides et al., 2020; Van Damme, 2017).

Secondly, the fact that trust in police was a strong predictor of the social acceptability of new SOSTs, highlights the importance of traditional 'in-person' policing. Police contact with citizens is a critical factor in determining the acceptability of new SOSTs. While technology and especially SOSTs are inherently impersonal and aim at detecting or deterring crime from afar, they also depend on individual interactions between citizens and police. In addition, a key function of (many) SOSTs is to improve efficiency and effectiveness, ultimately reducing crime numbers and increasing the rate of solved cases. It is no secret, that some policymakers also hope for a reduction in costs through this reduction of police demand. After all, this is one of the key functions of many of the smart city solutions presented in the field of policing (Straube & Belina, 2018). The increased reliance on technology and SOSTs for policing and crime reduction in the smart city might cut the interpersonal aspects as interactions with citizens are automated. While this development might save costs and improve crime prevention and detection, it may still have unintended consequences. Sindall and Sturgis (2013) for example find that less crime does not immediately create more trust. Instead, interaction between citizens and police is necessary to build relationships and ensure police have support and trust from the community. This is not only essential for more traditional policing approaches but also as a foundation for the use of SOSTs.

These findings highlight that the relationship between trust in police and the use of SOSTs is a complex one. On one hand can intrusive and socially less acceptable SOSTs damage trust in police and police-community-relations. On the other hand, trust in police was one of the most significant predictors of social acceptability and thus a good relationship with the police an important foundation of social acceptability of new SOSTs. This finding is especially important, carrying many policy implications. While automation in many aspects of our lives less personal by removing the human component (e.g., self-check outs in supermarkets), this is not a viable option in the field of policing and crime prevention.

6.5.4. Privacy Concerns

Both general privacy concerns as well as those pertaining to the government served as strong negative predictors of social acceptability. While privacy concerns about the government were significantly more impactful than general privacy concerns, both yielded negative results, indicating that individuals with high privacy concerns showed lower acceptability towards the new intervention.

These results are not too surprising but suggest that individuals clearly distinguish between the entities using their personal data. As mentioned in the previous chapter, the policing context matters. The question of who uses the data and which consequences this can create seem to be important factors for many people when thinking about being subjected to a new SOST. Considering that even individuals with low overall concern for the personal data stated that the use of data by the police would be problematic, highlights the importance of the law enforcement context. Thus, police forces that enjoy high trust from their community are less likely to face overt backlashes, but citizens may still question why data is collected and how it is processed.

Though there is a lack of reference point (i.e., how the use of data by the government or police compares to for example commercial users), the results indicate that though some respondents had high general privacy concerns, they still found the intervention acceptable. Individuals on the other hand, who were already concerned about the use of personal information by the government were highly likely to reject the intervention on the basis of its severe intrusiveness and overreach in terms of personal data and privacy.

These findings are, while not entirely surprising, novel to the academic debate as privacy concerns are primarily discussed in the context of online surveillance, not however, the use of SOSTs. Instead, authors such as Kudlacek (2015) find that video surveillance is largely positively received by the population and that most people assume a high crime preventive effect. In a comparison with the results of previous studies, however, his study finds that acceptance of video surveillance seems to have decreased somewhat in recent years (Kudlacek, 2015). The results of Kudlacek (2015) also suggest that the population is much more informed about the actual effects than is often assumed. There is no general expectation that video surveillance will provide effective protection.

This might be in parts attributed to greater sensitivities to privacy concerns regarding personal data, fuelled by several data breach scandals (Adams et al., 2017b; Murata et al., 2017a; Wilton, 2017) and the increased trade with personal information by big tech companies (Cohen & Mello, 2019; Smyth, 2019).

The findings carry several implications for policy making and further research. Primarily, they indicated that privacy concerns have to be treated seriously when deploying SOSTs as they have the potential to significantly undermine public support for the interventions. In addition, the findings suggest that interventions need to be transparent and follow clear privacy and data protection guidelines. Personal data needs to be kept safe and citizens need to be reassured to counteract possible negative effects of privacy concerns and concerns about the use of personal data by the government.

6.6. Conclusion

In summary, this the study found several significant predictors for the level of social acceptability of new SOSTs in the UK: trust in police, privacy concerns pertaining to the use of personal data by the government, political affiliation, as well as the impact of crime and fear of crime on individuals' lives. In addition, the intrusiveness of an intervention (i.e., how much and which data was gathered about individuals) and the level of automation (i.e., to what extent analysis and response were completed by AI) predicted the level of social acceptability well. While many people still hold positive views about video surveillance, these views are at least to some extent dependent on the characteristics of the intervention.

Many respondents showed concern over the usefulness and effectiveness of systems, meaning that improvements in these areas may lead to increased acceptability. However, this should not be used as a justification for continuously expanding the surveillance of private or public areas to a disproportionate degree. Ultimately, the use of the technology can only be justified by its direct benefit. Majority support and social acceptability are no free pass for increased surveillance. Neither do they overwrite important ethical and legal considerations that should be of paramount importance in any policy decision (see discussion in the following Chapter). Research on the acceptance of technology can therefore never provide legitimation.

Condensing the results, this study finds that social acceptability depends on three broad areas. Firstly, demographic factors and previous individual experiences impact the underlying attitude individuals have towards the use of new SOSTs. This study found that especially political affiliation and the impact of crime and fear of crime on one's life are strong predictors of the acceptability of surveillance measures. While the use of surveillance technologies may help to increase feelings of safety, this might not be the case for everyone as some people might be more likely to reject SOSTs depending on their political attitude or other personal experiences.

Secondly, trust in police and the government are important predictors of social acceptability. Individuals who do not trust police or have strong concerns about the use of their personal data by the government are significantly more likely to reject the use of new SOSTs. While this is unsurprising, it highlights the need for secure data storage and strong data protection policies. In addition, these efforts need to be communicated to avoid the spread of false information about surveillance measures and to ultimately increase public acceptability. Furthermore, trust in police was found to be a key predictor meaning that SOSTs cannot and should not serve to reduce or even replace police officers on the street. A good relationship between police and the community they serve is key for ensuring acceptability of new technologies.

The inherently distant and one-way nature of surveillance may in fact reduce trust in police meaning that existing efforts could be jeopardised by new systems. As such, it is essential that surveillance technologies are seen as a complimentary tool to patrols and a physical presence, rather than a replacement.

Lastly, especially two characteristics of the new technologies, discussed in the previous Chapter, predicted its social acceptability well, the level of intrusiveness and the level of automation. This highlights that there are red lines especially with regards to how much personal information a technology may collect and to what extent citizens trust the use of automated systems. While especially the use of AI may help to propel surveillance technologies from an after-the-fact intervention to a preventative technology, policy makers must be mindful not to create too much of a 'black box'. Surveillance must be transparent, and citizens need to know which data is collected and how it is used. This is not only crucial in normative terms and for several ethical issues but also practical reasons such as ensuring procedural justice.

As a result of these findings, a number of implications for future research and policymaking specifically in the UK arise which are discussed further in Chapter 7. As this study is entirely novel and had to some extent an exploratory character, it will be necessary for future research to validate the results and to further explore some of the nuances of social acceptability in this realm. As the relevance of the topic is only bound to increase and as the deployment of smart SOSTs will grow, policymakers should set clear boundaries and create a regulatory framework early on. This is a balance act as future policy needs to both protect individual privacy rights and allow police agencies to embrace technological innovation more readily.

Chapter Seven

Discussion: Opportunities, Challenges, and Future Scenarios

7.1. Chapter Overview

This final chapter summarises the main results of the research, highlights the contributions of the thesis to the fields of surveillance studies, crime science, and urban studies, and discusses implications of the findings for policymaking in the future, returning to the overall goal of this thesis: examining opportunities and challenges for crime prevention in smart city environments. The chapter then describes two concrete scenarios for the ethical and socially acceptable use of new SOSTs to tackle crime in smart cities. Lastly, the chapter discusses the limitations of this project as well as possible avenues for future research.

7.2. Contributions of the Individual Studies

This doctoral work aimed to identify and analyse practical opportunities and challenges for security and crime prevention associated with the use of smart city infrastructure. Each of the three presented studies (Chapters 3-6) contributes to this goal by examining a different aspect of the issue. What follows is a brief recapitulation of the opportunities and challenges identified in these studies.

7.2.1. Study 1 – Security Technologies and Their Functions in Smart Cities (Chapter 3)

As a first step, a systematic review was conducted, which examined the literature published in the last decade about new surveillance and security technologies in the realm of smart cities. The study focusses on the technological aspects, the architecture, and the functions of security technologies in smart city environments. With regards to the latter, it aims to investigate the extent to which these new interventions correspond to traditional functions of security interventions and how they affect urban planning and governance. To my knowledge, it is the first study to comprehensively review the literature on future security technologies and smart city developments. As such, it makes several important contributions to the literature and the academic debate. The most relevant contribution is the new classification for smart security interventions based on their functions that the chapter proposes. For this purpose, it merges two established frameworks, one with a focus on threat detection functions introduced by Borrion et al. (2014), and the other with a focus on crime prevention functions proposed by Ekblom and Hirschfield (2014). In order to advance these frameworks and to apply them in the smart city context, the resulting list of security functions is then applied to 121 smart city technologies. The three categories of security interventions in smart cities that emerged from this analysis are (1) those that combine new sensors with traditional actuators, (2) those that seek to make old systems smart(er) by either improving/automating processes or by managing and integrating the interplay between existing security solutions, and lastly, (3) those that introduce entirely new functions. This classification can help to group and compare interventions and to explore the distinct set of opportunities and challenges that they bring about. As such, it delivers a valuable addition to the conceptual landscape while aiming to give practitioners a tool to navigate the complex nexus that is surveillance and crime prevention in smart cities.

7.2.1.1. Opportunities and Challenges

Chapter 3 makes several additional contributions to the thesis. Firstly, it discusses what security technologies for smart cities exist and how the functions of smart technologies differ from traditional ones in the realm of crime prevention, laying the foundation for the subsequent chapters. The study finds that a wide range of solutions are available and asserted that crime prevention and surveillance in smart cities are not primarily or exclusively limited by a lack of technologies but rather the societal implications of their deployment and use. This constitutes an opportunity and a challenge alike.

On the one hand, the availability of innovative technologies to tackle urban issues means room to improve and make cities safer and more sustainable. On the other hand, the abundance of opportunities means that even greater focus needs to be placed on ensuring they are used responsibly and safely. To this extent, the study begs the question to what extent a poorly thought-through use of the technological possibilities might undermine individual privacy needs in the long run.

Secondly, the study highlights that not all systems need to be fundamentally new to become smart, and that building on existing infrastructure is crucial for successful smartification. This is especially true when optimising resource spending is a key aim of the smartification initiative and if resources for the smartification are limited. While the process of retrofitting cities and building smart systems on top of existing non-smart infrastructure might be a necessity in most scenarios, it also brings certain opportunities and challenges with it. The possibility to integrate new SOSTs within the existing infrastructure means new capabilities can be used to improve practice without lengthy adjustment periods or extensive training of practitioners. Such an integration requires the interoperability of technological solutions, which, as highlighted by the expert interviews in Chapter 4, is not always given. Furthermore, deploying new technologies within a wider framework of older solutions or to smartify existing infrastructure means that the deployment process becomes less resource-intensive but might also curtail the success of interventions, as smart technologies rely on integrating a wider network of sensors and actuators.

Lastly, the chapter emphasises that the implications of implementing new security technologies in urban spaces are far-reaching with regard to urban planning and governance. By analysing the functions of different technologies and discussing their overall relevance to the smart city, the study makes clear that future security infrastructures are not independent systems but a prerequisite for implementing smart systems across other realms of city services. This inevitable embeddedness of crime prevention and surveillance in the urban infrastructure is important for future smart city planning as well as policing and security. Thus, instead of treating security and crime prevention as the cherry on top of any smart city development, urban planners should consider it a core element of sustainable urban development.

Furthermore, this deep integration of surveillance offers opportunities for a holistic approach to crime prevention and policing. In particular, it promises better resource allocation, faster crime detection, and new possibilities to gather forensic data. These opportunities, however, come at a cost. This includes new ethical considerations and implications for the planning process itself. Questions of data ownership and privacy rights grow in importance and need to be reflected in contemporary planning processes.

7.2.2. Study 2 – Technological Innovation in Practice (Chapter 4)

In a second step, twenty expert interviews with practitioners in the fields of policing and surveillance were conducted to gain practical insights into the procurement, deployment, and use of new security technologies. This study focusses especially on opportunities and challenges, and the utility of smart and emerging digital technologies for crime prevention and policing. The primary aim of this part of the thesis was to better understand the priorities and perspectives of practitioners. The study discusses opportunities and challenges to the use of SOSTs in smart cities regarding practical procurement and deployment and day-to-day operations and institutional setups. Overall, it identifies three key areas for improving current practices of procuring and deploying new surveillance technologies for policing and crime prevention in London. These include insufficient institutional frameworks, issues of interoperability between different systems, and a lack of clear evidence-based guidelines surrounding social acceptability as a limiting factor.

This study is a valuable part of this thesis and important for the academic debate, as practitioner voices are rarely heard when it comes to the use of smart technologies for policing. The findings reiterate many of the results from the first study and contribute to a richer picture of smart cities and the ongoing debates on their likely risks and benefits. Interestingly, the results of this study only partially corroborate previous findings from the literature, especially with regards to the characterisation of police and crime prevention practitioners and their priorities in technological innovation. As such, this chapter adds a new perspective and highlights several ways to improve the current academic discourse. With regards to the latter, it shows several avenues for further research. Overall, the chapter contributes to a richer picture of practitioner perspectives, making novel contributions and creating new perspectives on existing research

7.2.2.1. Opportunities and Challenges

Chapter 4 finds that practitioners are often eager to expand capabilities. Many interviewees favoured increasing innovation and were actively bringing in ideas to use new technologies and improve service. Many were aware of institutional, social, political, or economic constraints and were critical of the usefulness of new technologies. Though the analysis of the interview data reveals some opportunities, especially regarding deployment scenarios, it more clearly points out shortcomings and institutional inefficiencies in the current system.

The study reveals that while in the theoretical and public debate, crime reduction is often seen as the standard measure of success, practitioners especially emphasised the need for better resource management tools. Here, new security and surveillance technologies could prove vital to counteract the negative impact of staff shortages and austerity measures. On the other hand, the study highlights the lack of clear rules concerning social acceptability and public opinion in the procurement, deployment, and use of new SOSTs. Often, boundaries are not clearly defined, and decisions are made independently from evidence on purely political grounds.

Furthermore, while the practitioners interviewed for this study were more prone to accept and adopt technology, a key problem remains that many public institutions (including police forces) are inherently bureaucratic and inflexible, which means they may not be able to keep up with the fast pace of smart city developments. While this inflexible nature of the institutions does to some extent ensure due process and accountability, it also means that public bodies have a harder time reacting to new technological developments. This issue is again reflected in the lack of interoperability between different systems, as described by several stakeholders. Rather than fully integrated systems, the deployment of new systems often limited the functionality of old ones, resulting in a more laborious processes for the users.

Lastly, the study raises the issue of public-private partnerships, which with regards to surveillance can have detrimental rather than beneficial effects. Though smart cities rely heavily on the harmonious interplay of private and public agents and the mutually beneficial use of each other's infrastructures (Ankitha et al., 2017; Choi & Na, 2017), practitioners did not find many benefits in the cooperation.

7.2.3. Study 3 – Exploring Social Acceptability (Chapters 5 and 6)

The final study conducted as part of this thesis is reported in Chapters 5 and 6. It highlights the issue of social acceptability and points to demographic and design elements associated with greater or lesser acceptance of SOSTs. The overall aim of the final study is to examine social acceptability as a challenge for using SOSTs to improve security in a smart city environment. The study consists of a vignette-based online survey that was conducted early 2021. By examining characteristics of the intervention and the population that might influence the acceptability of interventions, this study provides a starting point to evaluate future developments and derive policy recommendations for the procurement and deployment of SOSTs in the UK. Especially the demographic predictors explored in Chapter 6 are important to ensure SOSTs are deployed in a socially acceptable manner. In addition, this second part of the study, a structural equation model was used to identify the factors that may influence the level of acceptability of the interventions. Significant predictors identified in this study include trust in police, privacy concerns pertaining to the use of personal data by the government, political affiliation, the impact of crime, intrusiveness of an intervention as well as its level of automation.

Both chapters add to the conceptual understanding of the complex dynamics surrounding acceptability and helped to visualise how different factors contributed to it. Especially within the theme of smart cities, such an approach is novel and has to some extent exploratory character. Thus, the findings bring significant value to the current debate. The study especially highlights the importance of mediating factors including trust in police and privacy concerns in the formation of technology acceptance. In addition to advancing the conceptual understanding and providing policy recommendations for the socially acceptable deployment and use of new SOSTs in smart cities, the study also provides ideas for research to further explore the topic.

7.2.3.1. Opportunities and Challenges

While this last study was specifically designed to examine the social acceptability of the proposed interventions as a potential challenge, the results are nonetheless encouraging for the use of SOSTs in smart cities to detect or prevent crime. Even though more automated and more intrusive interventions are rated lower in terms of overall acceptability and are linked to increased concerns about privacy and abuse of the surveillance, they are nonetheless deemed to be overall acceptable. This highlights that there are red lines, especially with regards to how much personal information a technology may collect and to what extent citizens trust the use of automated systems.

In addition, the research demonstrates that most people favoured solutions with increased human involvement rather than the use of AI, contrasting previous studies (Klocke, 2001; Kudlacek, 2015). This means that not only the amount but also the type of oversight matters and can be seen as an opportunity to improve acceptability by increasing human involvement and ensuring due process when handling data.

The study further indicates that demographic factors and previous individual experiences might impact the level of acceptability of a new intervention. Especially political affiliation and the impact of crime and fear of crime on one's life are strong factors. While surveillance technologies may help increase feelings of safety, this might not be the case for everyone as some people might be more likely to reject SOSTs depending on their political attitude or other personal experiences. Furthermore, people with concerns about using their personal information by the government are likely to reject new SOSTs, especially in smart cities, where systems are likely more intrusive by default. These results once again highlight the importance of transparency and security when collecting and storing citizens' personal data. Trust in police is also an important factor for social acceptability. While it is unsurprising that people who are already untrusting of the police are likely to reject increased surveillance, the finding carries many important implications for deploying and using new SOSTs.

7.3. Implications and Recommendations

Exploring the nexus of surveillance and smart cities is important work to guide future developments. As this thesis demonstrates, both concepts are inseparably intertwined. Smart cities not only offer a range of opportunities for surveillance, but they rely on surveillance (though not always for crime prevention purposes) to ensure their functioning. At the same time, the smartification of cities will have such a lasting impact on the design of urban infrastructure that it will inevitably shape the future of surveillance and policing. As such, we can derive implications from the previously presented research findings of this thesis for both smart city developments and the deployment and use of new SOSTs. In the following, common themes from the three studies will be brought together and contextualised in the academic debate, discussing implications for surveillance and smart city planning. While some of the themes were central results of the presented studies, others were more peripheral. As one aim of this thesis is to contribute to the overall discussion surrounding the surveillance and security in smart cities, both types of results are important to discuss. Where possible, results will be discussed in relation to previous studies and real-life examples of smart cities.

7.3.1. Implications and Recommendations for Surveillance and Policing

The use of SOSTs in smart cities has a number of implications, both on a practical level as well as on philosophical and theoretical levels. Practically, smart cities will offer a range of opportunities for surveillance, crime prevention, and policing by improving existing functions and introducing new ones (see Chapter 3). From larger amounts of data to predict crime more accurately to the wealth of information offered for forensic analyses, nearly unlimited possibilities seem to exist for how to harness the data wealth of the smart city to increase safety and security. At the same time, these opportunities come with new challenges and potential pitfalls (as described above). Through the deployment of inexpensive and powerful surveillance systems, tackling crime might become cheaper and easier but they might also make providing meaningful oversight and ensuring justice and privacy for all citizens alike harder (Joh, 2019b).

7.3.1.1. Acceptability and Trust in Police

As discussed in Chapters 5 and 6, surveillance in smart cities conducted by or connected to police or other state security providers, especially when using AI, could lead to several issues for public trust and police-community-relations. Firstly, automating policing tasks through the use of direct actuators that deploy responses without human input means that part of the relationship between police and public will be offloaded onto citizen-machine-interaction.

The findings of this thesis echo previous research and once again highlight the danger of reduced trust in police. Citizens' trust in the police may suffer from the 'automation' of policing through CCTV surveillance unless additional staff are deployed (Smith, 2020). In the UK, acceptance of CCTV measures is generally high, but police presence is mostly preferred (Coleman, 2012, p. 203). The findings presented in Chapter 6 also suggest that direct, positive, contact with citizens ultimately earns the police more trust than the crime-reduction benefits of a technological solution.

Apart from the reduced interaction with the citizens, the deployment of smart SOSTs may also change other police activities, as the case of CCTV shows. While for some police forces in the UK the introduction of the optical-electronic equipment meant a relief, as in the case of West Yorkshire Police in Bingley (Gras, 2003, p. 219), others complained about the additional work of watching the monitors, analysing the data, as well as increased demand due to CCTV-related detections of crimes (Fay, 1998, p. 239). Similar issues were reported by practitioners in London as presented in Chapter 4, who voiced concerns about increased demand, additional workloads, and long training periods. Here, most SOSTs differ from traditional systems as due to the use of AI and increased automation they normally only require minimal human attention to be operated.

In addition, while hypothetically, the use of AI could mean increased fairness and more objective decision-making, it likely has the opposite effect in practice. As research indicates, there is a risk that algorithms may reproduce or even enhance bias which could lead to the wrongful accusation or even conviction of innocent people (Ammicht Quinn et al., 2015; Lee, 2018; Noor, 2020). Bias or even just the perception of bias amongst citizens has the potential to devastate trust in police and could increase resistance against all forms of police surveillance. A decline in police legitimacy may also lead to non-compliance with the law and reduced cooperation with authority (Sunshine & Tyler, 2003).

This would be highly problematic as this thesis demonstrates that low trust in the police and the government and concerns about data protection serve as important mediating factors and significantly influence the social acceptability of new SOSTs. This, in turn, means that a good relationship between police and the community they serve is key for ensuring the acceptability of new technologies. While this research finds that acceptance for both traditional and more intrusive smart systems is overall high, existing efforts could still be jeopardised by a too intrusive surveillance system, especially in places where the relationship between community and police is already strained.

To counteract this, several studies argue that surveillance should be transparent, and citizens need to know what data is being collected and how it is used (Dix, 2016; Nesterova, 2020; Omrani & Soulié, 2020; Purtova, 2018; Winkler, 2011). Not only is this crucial in normative terms and for several ethical issues but also for practical reasons such as ensuring procedural justice and maintaining and fostering trust in police. In addition, this thesis emphasises technologies must be tested to ensure that potential bias is as low as practically possible and that systems are reliable enough for deployment. Thus, policymakers need to create clear and rigorous oversight structures to anticipate challenges and unintended consequences such as possible blowback and implications for police legitimacy and police-community relations.

7.3.1.2. The Nature of Policing

Not only the relationship with citizens might be impacted by the increased smartification of urban spaces. The dynamics created by smart cities and growing privatisation also have the potential to change the very nature of policing that takes place in the city. Because smart cities are aimed at ensuring a smooth operating of urban services and flows of people, they aim to avoid disruption at all costs. As such, smart city policing might emphasise what Shearing and Stenning (1985) referred to as 'Disney policing', i.e., willing cooperation rather than coercion through guns, batons, or handcuffs (Joh, 2019b). The approach aims to be 'embedded, preventative, subtle, cooperative, and apparently non-coercive and consensual' (Shearing & Stenning, 1985, p. 304). In many respects, Disney policing describes many practitioners' ideal case of policing in the smart city. It relies heavily on control strategies embedded in the environment and requires less active intervention.

Similar to the smart city, control structures in Disney World also have further functions that overshadow the control function. Shearing and Stenning (1985) describe for example how water features and flower beds serve as aesthetic objects but also do direct visitor flows and how even though most employees are engaged in other activities, all of them are also there to maintain order. In smart cities, this is also the case. Elements of the urban environment might serve other primary functions but contribute in part to the overall maintenance of security and order. Through this, control functions are embedded in the fabric of the city so that their presence is unnoticed, but their effects are visible, allowing coercive practices to be reduced.

Though such developments might not be undesirable altogether and might have benefits for trust in police, both positive and negative unintended consequences are important to anticipate. Opportunities for better policing in smart cities should be considered from the onset of any new developments but need to be critically evaluated against evidence base and possible risks to liberties and privacy.

In the case of Disney, the subtle, non-coercive, and consensual nature of the system relies heavily on two factors. Firstly, Disney world is a private space where although control mechanisms are disciplinary, they are non-carceral and ultimately determined by Disney Productions rather than the moral or absolute. Secondly, individuals subjected to the pervasive surveillance at Disney want to maintain access to the space for breaking the rules may result in expulsion from Disney World altogether. Thus, even though there may be some benefits associated with such a style of control and security, it ultimately relies on exclusionary practices that are not suitable to implement in public urban environments.

7.3.1.3. Public-Private Partnerships and Policing

Another common thread throughout all chapters of this thesis is the question of public-private partnerships. In the academic debate around smart cities, this issue is discussed from various perspectives and either framed as a great opportunity or the biggest threat to urban life and civil liberties. Often, however, studies maintain that the smartification of cities necessarily brings increased privatisation with it. This is due to the fact that deploying SOSTs as part of a fully integrated and comprehensive smart city requires various technological advancements that are necessary to make sense of the immense amounts of data, such as improved algorithmic analyses methods. Such advancements will, for the most part, be created by private companies. This means that much of the smart city technology is privately developed products sold to public (and private) customers (Joh, 2019b).

As a result, policing will rely increasingly on public-private partnerships, as embedding policing in the smart city means embedding it in an infrastructure that is both public and private (Joh, 2019b). In addition, increasing automation, which is a key feature of most smart technologies, also means increased reliance on and influence of private interests (Wexler, 2018, p. 1349). While such partnerships may be useful to some extent as they can save costs and make processes faster and more inclusive, they can also create new challenges to crime prevention and policing efforts, as discussed in Chapter 4. Practitioners interviewed in this thesis emphasised the danger for security and policing efforts when partnerships fail or do not benefit the public because economic interests of new developments have been prioritised. While this thesis only reports small-scale examples of issues in public-private partnerships, many other examples exist that highlight the danger of failing partnership arrangements. Especially the recently failed Toronto Waterfront project has been portrayed as a heap of miscommunication and broken relationships between the municipal government and Alphabet Inc.'s Sidewalk Labs (Carr & Hesse, 2020).

Increased privatisation of infrastructure might, however, also have implications for the nature of policing and security taking place in the city if relationships function well as they might mean an increased reliance on private security personnel for daily surveillance work in joint projects between the police and the private sector. This privatisation of surveillance work is not without problems: the inconsistent qualifications of private service personnel are difficult to verify. In addition, the police's own rules do not necessarily apply to the privately hired security guards, so that the daily monitoring activities might not follow basic legal requirements as less or no public accountability exists. In addition, privatised surveillance of cities brings up many questions about data ownership and governance which need to be addressed (Austin & Lie, 2021). As Chapter 6 demonstrates, privacy concerns are hugely important predictors of social acceptability and thus need to be considered in agreements between private and public bodies. Here, policymakers need to ensure that partnerships are set up to benefit the public and that private infrastructure is available to serve public needs.

7.3.1.4. The Pitfalls of Automation

Building smart cities also inevitably brings about another change for policing that has been mentioned on several occasions throughout this thesis, namely the increased reliance on automation which might make policing more instantaneous. Automated enforcement describes when AI automatically deploys actions if unwanted behaviour is detected. For example, the town of Maidstone, UK, has recently started to use an AI system to automatically detect and fine motorists who litter (Hellen, 2021), while in Shenzhen, China, a smart system automatically and immediately fines anyone jaywalking (Mohsin, 2020). While automated enforcement is in itself nothing new and already finds application in tax and traffic speed monitoring (Petit, 2018; Wells, 2008), smart cities may see this automated enforcement on a much larger scale for a wider variety of crimes. As mentioned before, this thesis touches upon this issue in several chapters. It has, however, yet to discuss the benefits and pitfalls of such a system. One side-effect of algorithmic decision-making and the automated deployment of responses is that it creates a zero-tolerance enforcement policy, where crimes or unwanted actions are punished as soon as they occur, regardless of the situational circumstances. While such a (near) 100% detection and punishment rate may sound positive at first, it is critical to consider societal consequences and unintended effects. Firstly, the results of the study presented in Chapters 5 and 6 indicate that the effectiveness of an intervention in terms of crime reduction is likely not a significant predictor of the acceptability of a new SOST. Most citizens prefer contact with the police over mere interaction with a technology – at least in scenarios where they are not the subject of investigation. This is further supported by authors such as Taylor and Lee (2019) and Clare et al. (2019) who find that a majority of arrestees is concerned about manipulation, modification, and misrepresentation in body-worn camera footage or even CCTV. Here, the fault lies (at least in the cases described in the research) within the interpretation and handling of footage by officers rather than the technology itself.

Other research suggests that it is questionable whether a zero-tolerance enforcement policy would yield the desired effects, namely a change in behaviour by a majority of the population. Wells (2008) finds that this is exactly the case with traffic speed enforcement. While the automated issuing of tickets is far more efficient, most motorists rejected the practice, arguing it was too impersonal and did not consider situational factors (Wells, 2008). Even though humans are less efficient, they are more capable of ethical and contextualised decision-making than automated systems (Hartzog, Conti, Nelson, & Shay, 2015).

Hartzog et al. (2015) argues that many of today's laws are not created to be automatically enforced as they purposefully leave room for interpretation and leniency and Petit (2018) maintains that 'some degree of discretion is inescapable to execute law'. As such, this thesis argues that the apparent benefits in terms of efficiency and resourcing need to be treated with caution and potential negative side-effects assessed. In the worst case, automated enforcement can lead to a rejection of law enforcement and damage police-community relations (Joh, 2007).

7.3.1.5. Procedural Justice and Due Process

The potentially drastic changes to policing and automated enforcement, described in the previous chapters also have a number of implications for some of the most basic principles of good policing and fair criminal justice. Practitioners should, for example, ask the question what the automated response to unwanted behaviour such as the automatic triggering of actuators in the city or automatic fines for illegal behaviour (e.g., littering, speeding) means for procedural justice. Questions of what happens when urban infrastructure itself controls crime or makes some forms of crime impossible are not only important for discussions of ethics but need to be faced by policymakers. Can automated processes ensure a fair process, and can automation distinguish between different scenarios?

While there are certainly some benefits in terms of demand management, many authors paint a negative picture of automated enforcement practices in smart cities. Individuals perceived to be offenders by an automated system could be barred from entering certain places[20] (Joh, 2019b), autonomous robots might deploy stun guns if deeming citizens a threat (Lin & Singer, 2016), and autonomous cars might make it impossible to speed or run red lights without being able to fully judge every situation (Joh, 2019b). If done right, such systems might improve security and safety for all; if not, they might undermine fundamental principles of democracy and the rule of law. Especially the automation of decision-making preceding the restriction of a certain action, or the deployment of a response measure is problematic. On several occasions, this thesis warns of the creation or use of 'black boxes', which

[20] While similar practices already exist that ban sex offenders or shop-lifters from certain places, such measures are usually the result of a conviction and put in place by judges rather than an AI.

specifically applies to the decision-making processes of AI but also to most other technological solutions to crime. Especially with the growing inclusion of AI and machine learning in SOSTs, there might be growing uncertainty about how the technology reaches its decisions, leading to severe implications for transparency and procedural justice (Bennett Moses & Chan, 2018).

At the same time, the use of new SOSTs in smart cities offers opportunities to improve fairness and justice. Such opportunities are, however, only possible if due process regardless of the level of automation and technological sophistication of the interventions is ensured. This can be done through human oversight or the possibility of plausible reasoning by the system (Sunshine & Tyler, 2003).

As the relevance of the topic is only bound to increase (Haggerty, 2004; Patterson, 2004; Seddon, 2004) and as the deployment of smart SOSTs will grow, policymakers should set clear boundaries and create clear legislation early on.

7.3.1.6. Changing the Foundations of Surveillance

While the primary goal of this thesis is to explore the opportunities and challenges of smart city technologies for crime prevention and surveillance, it also contributes to theory development. In particular, the findings have important implications for the theoretical underpinnings and philosophical concept of surveillance. The deep embeddedness of surveillance (here in the sense of crime prevention and deterrence) in the wider urban infrastructure changes several fundamental aspects of its functioning. The first one is that the inclusion of actuators and the use of AI introduces feedback loops that are not a part of traditional surveillance systems. This shifts the debate significantly, as surveillance is suddenly no longer considered a one-way exercise between watcher and observed. Instead of the panoptic uncertainty described by Bentham and Foucault (Galič et al., 2017; Parreno & Demeterio III, 2012), individuals subjected to the surveillance system know that they are always being watched as a decentralised camera system or an AI always 'watches' and analyses each feed in real-time. While one might hypothesise that this only increases the disciplinary effect of the surveillance, it might also contribute to the opposite.

In the panoptic surveillance scenario, the observed is unaware whether his actions did not trigger a response because he happened not to be watched in that minute or whether the action was deemed acceptable.[21] In the smart environment where individuals know that they are being watched, a lack of immediate feedback, i.e., no triggering of an actuator, may be understood as the action being acceptable. As such, a fundamental tenet of the philosophical concept of surveillance changes, shifting the debate away from the focus on uncertainty towards the question of what happens if constant surveillance is not only a possibility but a non-negotiable reality. While this thesis does its best to capture the nature of comprehensive smart SOSTs and measure what predicts their social acceptability, policymakers need to be aware that the results of such fundamental changes are hard to foresee.

This is especially the case with the ubiquity of surveillance in the smart city context. As a tool of social control, surveillance technologies are often discussed as factors that increase feelings of insecurity (Watzinger, 2019). According to Watzinger (2019), these feelings of insecurity can often be traced back to the technological decentralisation of surveillance, as often the case in smart cities. This decentralisation means the disappearance of visible control, i.e., it is no longer clear who is being monitored, when and for what purpose. Reichardt (2016) and Watzinger (2019) also suggest that the changes to surveillance in the smart city context constitute a multiplication and condensation of surveillance. Surveillance becomes diffuse and less strategic, and as it is so all-encompassing, the boundaries of surveillance blur and merge. The spread of surveillance to other technologies and aspects of urban life, initially not focussed on surveillance, is what the literature calls

[21] It may also be the case that resources are not available. This is, however, irrelevant as the observed does not know why no response follows an action as he is in the constant state of surveillance.

'surveillance creep' (Fussey, 2007). Policymakers and practitioners need to be aware of these possibly shifting boundaries and should aim to set clear confines to prevent surveillance creep.

7.3.2. Implications and Recommendations for Smart City Design

The results of this thesis also have several implications for the design of smart cities in the future. As also discussed in the previous section, a range of technological solutions are available to tackle all problems of urban life today, including issues of insecurity and crime. As such, developing smart cities is, for the most part, not a question of the availability of technologies but one of finding appropriate solutions that solve problems adequately while respecting privacy and civil liberties. Ultimately, the implications for surveillance and policing and those for smart city design are, to some extent, two sides of the same coin. This thesis identifies both benefits and drawbacks with regards to using the smart city environment for surveillance. Especially the latter is the case for issues of privacy protection and social acceptability. Here the nexus of smart cities and surveillance has a circular character as smarter surveillance that promises many benefits for policing only works if citizens have sufficient trust in police and find interventions acceptable. This acceptability is, however, undermined by more intrusive interventions.

7.3.2.1. Social Exclusion as an Unintended Consequence

While the use of smart city sensors and infrastructure for the purpose of policing and crime prevention can have several benefits for police, it may also produce unintended consequences for citizens and smart cities as a whole. This includes especially the furtherance of social exclusion and discrimination.

That surveillance practices can be unfairly discriminatory is nothing new, as Norris and Armstrong (1999) point out that surveillance work in control rooms is often carried out selectively. Stereotypes based on gender, skin colour, or clothing are often reproduced and influence who is targeted by surveillance (Graham, 1998;

Wehrheim, 2012, p. 91). Personal prejudices of operators often influence the interpretation of certain behaviours and for the classification of persons. The decisive factor for selection is often not the behaviour itself, but the appearance of those under surveillance, which can be associated with a certain (undesirable) pattern of behaviour (Wehrheim, 2012, p. 91). As this thesis discussed on several occasions, stereotyping and biases are often also present when using AI and automated systems. As such, video surveillance not only serves as a means of preventing security incidents, but in most cases inevitably leads to the exclusion of individuals and discrimination against certain social minorities that do not pose a direct threat to society but are perceived as such by the majority of the population. These mechanisms once again echo the concept of military urbanism, first discussed in Chapter 2, which suggests that the use of urban infrastructure for security purposes can lead to social division and discrimination (Graham, 2009; Iveson, 2010).

7.3.3. Ensuring Fairness in Public-Private-Partnerships

Such exclusionary practices link directly to the increased involvement of private partners in the design, creation, and administration, which also has important implications. While the widespread use of SOSTs by police may in some instances be justified by crime and the security needs of citizens, private interests are more focused on making locations safer and more attractive for residents and consumers. In this context, SOSTs serve to provide a feeling of safety and a pleasant atmosphere for consumers and potential customers, while deterring 'undesirable fringe groups' such as rough sleepers or drug users (Wehrheim, 2012, pp. 91-93). Such exclusionary practices raise many questions about the ownership of public space. While these questions are already relevant today, they will gain significance in the future because smart cities rely to a greater extent on private infrastructure than traditional urban spaces.

To address these concerns of inequality, policymakers need to ensure smart cities are, as the definition used in this thesis suggests, ‘citizen focused’, i.e., open and inviting environments for all citizens. It is important to ensure explicitly that diverse groups of people have access to all facilities and are not targeted due to external or behavioural characteristics. Furthermore, while the creation of safe and inviting environments should be in the interest of all, it should not lead to the exclusion of groups deemed ‘unfit’ by private business interests.

The increased influence of private interests may also impact the procurement of smart city components and technologies, companies might seek to ensure customer loyalty or dependence on their products (Joh, 2017b). This was a concern also expressed by stakeholders interviewed in Chapter 4. Especially where existing infrastructure is being retrofitted, private solutions might be more attractive than costly public projects. In the Spanish city of Jun, for example, citizens can use Twitter to do everything from filing crime reports to booking appointments in municipal services (Morales & Rubio Sánchez, 2017). While the project so far has been a success in reducing administrative burdens on the municipality and the local police, it has also made the city to some extent dependent on the tech giant. To avoid this, policymakers need to ensure flexibility and great enough competition to enable low costs and the greatest possible benefit for the public.

Furthermore, as trust in the security of one’s own personal information that are collected in the smart city is key to ensuring public acceptability of surveillance, deciding on appropriate data governance structures is key. While many different suggestions and models exist, even the most promising solutions, such as the Urban Data Trust created as part of the recently failed Toronto Waterfront development, have attracted significant public criticism (Artyushina, 2020; Austin & Lie, 2021). As such, bespoke solutions are required, that ensure the greatest possible utility of the collected data while protecting personal information and ensuring as much privacy as possible.

7.3.3.1. The Issue of Retrofitting

As discussed throughout this thesis, most cities in the UK and Europe aspiring to become smart cities of some kind have to retrofit their existing infrastructure. This process can save costs and help to ease the transition for both operators and citizens alike. It might, however, also lead to issues of compatibility, where new and old systems are not interoperable in practice and thus cannot be used to their full potential. Compatibility issues may also occur between smart technologies procured from different suppliers. These issues, as highlighted by many practitioners (discussed in Chapter 4), are especially problematic in the field of policing and crime prevention but apply to all areas of urban life. Because in the smart city all services are heavily interconnected, compatibility issues at only one place can mean significant parts of the system do not function as intended. Here, practitioners and policymakers, especially on a local level, need to ensure that new systems are able to communicate with one another and that compatibility is ensured not only within individual realms of city services but across all.

In addition, current administration structures are likely to hinder the effective and efficient deployment of new SOSTs. This is especially the case in the UK, where the fragmentation of police forces and local administrations and councils often leads to a lack of interoperable systems across local administrations. These problems are once again already known and have been highlighted both in Chapter 4 and in real life examples of smart city projects. The latter includes South Korea's Songdo Business District, often dubbed 'the world's first smart city' (Yoo, 2017). While the project was overall less successful than expected, some developers stopped putting out updates for apps relevant for using some of Songdo's smart services (Yoo, 2017).

7.3.3.2. Safety and Security as a Foundation

As discussed in Chapter 2, smart cities describe cities that use ICTs and all other technologies available to improve the effectiveness and efficiency of city services in order to save resources and to improve the quality of life for citizens. In order to meet the expectation of increased quality of life, smart city developers need to consider not only the final goal of a (nearly) crime-free and safer urban environment but also maximise questions of liberty and privacy in their designs in order to enable citizens to lead good lives. Here, practitioners should consider the aforementioned points on the dangers of automated enforcement in smart cities and should ask the question what kind of urban environment they want to create. As highlighted in Chapter 4, strategies that promise the most effective reduction of crime might not be those best implemented due to unforeseen consequences. This is further supported by the literature as Wells (2008) who discusses traffic speed enforcement suggests that the goal should be to dissuade or deter offending behaviours rather than to reach 100% crime detection rates. As such, police and other security services need to be included in the planning of smart cities to anticipate risks and maximise the utility of new infrastructure.

At the same time, Chapter 3 highlights that security and safety should not be seen as separate issues but rather as a prerequisite for any smart city. To unleash the full potential of the smart city crime prevention concept, security and safety need to be engrained in the fabric of the urban environment and be considered as foundations in the planning process. Thus, integrating crime prevention fully in the smart city design requires a new way of thinking about how cities are planned and implemented. This should be done in a positive manner, ensuring equality and focussing on citizen needs rather than social control (Vitalij et al., 2012). This echoes the Safe City concept introduced in the beginning of this thesis as well as approaches from the literature. Chiodi (2016) suggests that security and crime prevention aspects should be evaluated as underlying conditions for every urban planning and design project.

This thesis identifies benefits of using smart city infrastructure for surveillance purposes and stresses that security and safety functions should be embedded in smart city infrastructure. Nonetheless, clear boundaries need to be set to ensure privacy rights and prevent an unnecessary securitisation of processes as emphasised in Chapters 5 and 6.

7.3.3.3. Streamlined and Evidence-Based Administration

This thesis highlights that practitioners face, in many instances, bureaucracy and lengthy and inflexible processes that make the procurement and use of innovative technologies slow and cumbersome. While in the spending of public funds, some bureaucratic process is necessary, it does not create a fertile ground for innovation as the interviews reported in Chapter 4 discuss. This study further shows that decision-making often seems to be arbitrary and not based on evidence, especially with regard to acceptability thresholds of new SOSTs. As such, this thesis recommends that policymakers improve and streamline existing decision-making and procurement processes to adapt to the pace of technological innovation and to make cities future ready. Individual assessments of new technologies are necessary to ensure public support for new interventions. This is especially necessary as the rejection of surveillance in the realm of crime prevention may also spill over to other city services or because function creep could lead to the use of data from other services such as waste management by the police (Joh, 2019b). In fact, a number of smart city projects, most notably including Toronto's Waterfront development, have failed because public resistance grew too big or because community trust was missing from the onset (Mann, Mitchell, Foth, & Anastasiu, 2020).

7.4. Scenarios for the Responsible Use of Smart Surveillance

Thus far, the chapter has summarised the findings from the three studies as well as the resulting implications and recommendations for future surveillance and smart city policy in the UK. The question remains, however, how systems can harness technological possibilities to improve policing and crime prevention, while ensuring an ethical and responsible usage that does not violate the privacy of those subjected to the system. To answer this question and to further illustrate the findings of this thesis, two possible use cases are described in the following. Scenario 1 focuses on potential negative impacts of surveillance for trust in police and police-community-relations. Scenario 2 proposes a system that emphasises data protection while maintaining even the most intrusive surveillance functions. Each of the scenarios highlights a specific aspect or best practice, meaning that they are not mutually exclusive but can be combined for best fit.

7.4.1. Managing Demand and Improving Police-Community-Relations

There are various suggestions for harnessing the opportunities that the close integration of policing and surveillance in urban infrastructure offers. One of these suggestions is moving away from using surveillance for deterrence and emphasising the third function of SOSTs, namely the management of resources. Such a system places an increased focus on increasing procedural justice and trust in police and improving police-community relations. Especially in the context of smart cities, which by design require increased reliance on automation and technology, it feels almost counterintuitive to focus increasingly on the human component. This contrasts the notion of increased automation in policing or what McGuire (2020) calls the 'end of policing' as we know it.

7.4.1.1. Trust in Police and Social Acceptability

Because trust in police is best fostered through (positive) in-person interaction between officers and citizens (Van Damme, 2017), this scenario highlights the need for the increased physical presence of officers. In doing so, this scenario does not argue that the use of automated SOSTs in smart city environments is not useful. Instead, it seeks to emphasise that the resulting implications of more ample opportunities for surveillance do not need to be harsher, more intrusive, and less community-oriented policing.

As discussed on several occasions in this thesis, a lack of social acceptability can quickly lead to a deterioration in police-community relations and trust in police (Wells, 2007). This effect is even greater if the relationship between police and citizens is already strained or with individuals who are disproportionately affected by crime and fear of crime (Kochel, 2018). Trust in police and government and previous experiences with the police form a foundation for the social acceptability of new SOSTs. The idea behind this proposal is to use surveillance and the significant amounts of data not for person-specific surveillance but rather to improve police resourcing. Instead of tackling crime directly, such a system aims to address the inefficient use of resources or the lack of resources by deploying them more efficiently. Smart cities create opportunities to counteract the negative effects of austerity and resource shortages, while at the same time helping forces to address police demand better. Through the wealth of available data, police forces will be able to better predict demand for services and plan resource spending accordingly. Thus, smart cities allow police management to take a more proactive and future-oriented role. The system thus does not aim to reduce personnel cost overall but rather to reinvest saved resources to engage with citizens and improve trust in police and police-community relations.

Given that the transformation to the smart city often requires significant physical changes and redesign of urban infrastructure, this approach could be coupled with increased use of CPTED principles in the design of future cities. This could lead to a reduction of crime and thus overall police demand, freeing up further resources. Here, surveillance systems could have a double function. Firstly, they could, as described, allow for increased police patrols, which aim to increase the most valuable asset of police, citizen consent and cooperation, through direct contact (Silverman & Della-Giustina, 2001). Secondly, the systems could serve to improve guardianship by making citizens feel safer and increasing foot traffic, i.e., eyes on the street and natural surveillance (Gill & Spriggs, 2005; McLean et al., 2013; Spriggs et al., 2005). In the sense of the latter, this means especially visible systems would be useful that are physically present and improve the feeling of safety (Rothmann, 2010).

7.4.1.2. Use Cases and Real-Life Examples

SOSTs, especially with the focus of engaging with the community and improving the feeling of safety, have shown to be in some instances a vital part in revitalisation efforts for crime-ridden and otherwise socially disadvantaged neighbourhoods (Klauser, 2007; Wheeler, 2016; Wiig, 2018). An example of this is the case of Camden, New Jersey. There, an integrated smart city strategy that included security and crime prevention efforts as a foundational element led to the revitalisation of the city (Wiig, 2018). The historically crime-plagued city tackled their issues with a data-driven policing strategy that allowed officers on the street to operate in tandem with a control room monitoring the city (Wheeler, 2016; Wiig, 2018). Police and local administration relied on the dual effects of managing resources and engaging with citizens, and the success of this strategy meant not only that crime was falling but also that other smart city initiatives in the realms of transportation and waste management could be realised, attracting further outside investment (Wiig, 2018). This, in turn led to higher citizen engagement, the revitalisation of entire neighbourhoods, and more significantly falling crime numbers, even in areas that were not directly affected by policing initiatives (Wiig, 2018).

This means that security and crime prevention can create the foundation for revitalisation efforts but need to be accompanied by social, housing, and city planning strategy to ensure the creation of new districts to attract multinational knowledge and innovation-focused industries (Cretu, 2012; Wiig, 2018).

The scenario described here emphasises the citizen-focus of smart cities and highlights the need for human interaction as an underlying criterion for the success of smart cities (Cardullo & Kitchin, 2019; Mandl & Schaner, 2012). The approach puts a focus on the goal of smart cities to make the urban environment and infrastructure reactive to the presence and needs of citizens (Vanolo, 2014, 2016).

7.4.2. A Privacy-Delimited System

Alternative approaches to security that integrate CPTED and community policing as described in the first scenario are, however, neither always suitable nor always part of the political agenda or wanted by practitioners or citizens. As such, the second scenario describes the case of a fully integrated SOST deployed in the smart city of the future. This hypothetical system has all possible capabilities and as such comes with a range of drawbacks in terms of social acceptability, privacy protection, personal liberties, and ethics. The following will thus describe a method that, while not addressing all concerns, might help to make the system and its use more ethical and socially acceptable. The option described here is a multi-level privacy-delimited system based on the principles of the 'privacy by design' concept first introduced by Cavoukian (2009b). The core idea behind such a system is that while practitioners have all technological solutions at their disposal, they can only be used if certain situational criteria are satisfied, and potential criminal action has been detected.

7.4.2.1. Practical Design of the System

Practically, the system combines surveillance technologies with privacy-enhancing technologies to implement data protection through technical procedures. Roßnagel, Desoi, and Hornung (2011) offer a starting point for such a system that is not only socially acceptable but conducive to the responsible and proportionate deployment and use of surveillance infrastructure. They discuss a method by which only some functions of a smart surveillance system are available all the time while others can only be used for instances where a crime is suspected or has occurred. This is done to maximise privacy while allowing for the benefits of smart surveillance in terms of crime detection and prevention. To achieve an appropriate balance between security and freedom, a three-tier model is suggested. In the first stage, the system is severely limited in its power and only basic functions are available to the operator to observe the monitored area. The aim of this level is to give the operator as good an overview as possible without interfering with the rights of the observed. To protect privacy, the videos shown to the operator can be protected by suitable image manipulation methods, such as pixelation. The change to the second stage occurs either automatically, i.e., when an algorithm observes suspicious behaviour, or at the direct request of the operator. In the second stage, i.e., if an illicit activity is suspected, more intrusive procedures are available for assessing the situation. For example, the operator can now zoom in on cameras at will and make use of advanced algorithms, such as automatic people tracking. Even at this stage, the right to informational self-determination of the person being observed should be preserved as far as possible. The system continues to avoid displaying the face of the person concerned and does not allow the extraction of biometric templates that could be used for later personal recognition. The change to the third stage can again be made by an algorithm or at the request of the operator.

In the third stage, it is highly likely that a criminal offence has been committed or that a concrete danger exists that can only be averted by the intervention of security personnel. It is primarily used to preserve evidence and to coordinate with emergency forces on site. The video surveillance system now also reveals the faces of the persons concerned and allows the operator to extract a biometric template, which can also be used for person identification. The application proposed by Roßnagel et al. (2011) clearly demonstrates how the power of the system, and thus also its potential encroachment on the rights of those affected, can be compared with the current situation. If a situation threatens to escalate, it justifies deeper intervention but limits this to a certain amount of time and a small group of people.

7.4.2.2. Need for a Regulatory Framework

While the application of a privacy-delimited system could ensure that drawbacks in terms of privacy and civil liberties are reduced, it does not eliminate them entirely.

In addition, with increased reliance on AI, such a system could be biased, meaning that certain groups are more often subject to surveillance than others (Noor, 2020). These potential issues highlight that no perfect system for surveillance exists and that trade-offs between privacy and security are (at least with regards to public surveillance) still a real issue. The use of a privacy-delimited system as a technological compromise does, however, need to be accompanied by appropriate legislation. Such legislation should aim to create a balance between the requirements of electronic data processing in governmental and non-governmental contexts on the one hand and the protection needs of individuals and their personal rights on the other (Kammerer, 2016). As legislative initiatives are often late in relation to developments in information technology, they require an extraordinary amount of foresight and anticipation. In addition, current inconsistencies of data protection legislation at the local, regional, and national levels need to be addressed (Kammerer, 2016).

In addition, to further even the scales between observers and observed, governments need to implement a strong duty of all data-processing institutions (governmental or non-governmental) to provide information to data subjects on request about what personal information they hold about them. This obligation also extends to visual information, e.g., recordings from surveillance cameras.

Such a freedom of information policy, as it is already in place in the UK, should not only include the raw data but also information about how data is processed and on what basis decisions are reached (Degeling, 2014).

7.5. Limitations and Avenues for Future Research

This thesis has provided important insights into the use of SOSTs in smart city environments and provided valuable recommendations for practitioners and policymakers. Nevertheless, there are a number of limitations that arise from the design of individual studies and this thesis as a whole. The following section discusses these limitations and presents avenues for future research.

One key limitation that was acknowledged on several occasions throughout this thesis is the limited transferability of the findings as they may depend heavily on the national context and the socio-cultural environment within which the research was conducted (Menichelli, 2014). As the literature suggests that attitudes between regions and countries may differ greatly, specifically with regards to the use of new SOSTs (Banisar & Davies, 1999; Brandl et al., 1994; Norris et al., 2004; van Heek et al., 2017), it would be useful to see to what extent the findings presented here can be applied abroad. For this purpose, two kinds of evaluations come to mind. Firstly, it would be interesting to explore the extent to which the results can be generalised and whether something like an international or at least regional baseline for social acceptability of new SOSTs can be found. As such, comparison studies should be conducted in other socio-cultural contexts. Secondly, research examining the implications of the installation of new SOSTs in environments with currently and historically less surveilled societies might help to determine the importance of cultural factors and provide further insights for developing proactive approaches for policymaking in this field.

Another point is that this thesis provides policy recommendations rather than concrete design guidelines or system architectures. This choice reflects the previously mentioned iceberg of issues associated with crime prevention and surveillance in smart cities. There are many scientific engineering papers on the subject of smart video surveillance. They often focus on the acquisition and evaluation of image data or scaling system architectures. The question of how to increase the acceptance of these systems is only examined by a few groups, whereby this is almost always to be achieved through increased anonymisation. The engineering literature can further be divided into two sub-groups. On the one hand, work that deals with the protection of video data, and on the other hand, work that looks at the design, development, and deployment of overall systems. While this is obvious – after all, the biggest criticism of (smart) CCTV is regarding privacy – it does not cover the full range of issues, especially those of more practical nature such as implementation frameworks and institutional realities. Once again, there is an abundance of specific technological solutions, while general principles that guide the deployment are missing, a gap that this thesis addressed. Nonetheless, it would be useful to apply existing studies to the smart city context. One example of a concrete list of recommendations for the socially acceptable design of SOSTs has been introduced by Nissen (2014). Adapting the framework by Nissen (2014) for the smart city context and combining these results with the relevant recommendations from this thesis would provide a comprehensive frame on both the policy and technology level for socially acceptable SOSTs in smart cities.

Another limitation of this thesis is that while it was only able to show the existence of red lines that may not be crossed if interventions aim to be acceptable, it could not fully locate where exactly they are drawn. Though especially Chapters 5 and 6 offer insights into the factors that can impact social acceptability, the findings suggest that the context of the deployment of new SOSTs matters greatly and that individual evaluations of social acceptability for each project are vital. Here, once again the before-mentioned recommendations by Nissen (2014) can serve as a foundation. Nonetheless, risks of social acceptability need to be considered, and citizens should be consulted on the deployment of SOSTs to ensure maximum cooperation and acceptance within the population. Future research should consider the creation of a standardised framework, the foundation of which can be found in this thesis.

While the scenarios described in the previous section offer a starting point for socially acceptable surveillance that respects individual privacy rights, it is important to recognise that such approaches only cover part of what the smart city is. It is for example also important to keep an eye on developments in the private sector, especially since smart cities rely in many areas on private infrastructure (Liu et al., 2020b). This means that formal government surveillance will be increased and that many private businesses will rely more and more on automated surveillance mechanisms. Like the smart city, private businesses will use automated facial recognition and other sensors to streamline and improve their services.

A prime example of this is the concept of Amazon Go, a checkout-less supermarket that entirely relies on sensors and facial recognition to bill customers for their shopping (Huberman, 2021; Wankhede, Wukkadada, & Nadar, 2018). Here surveillance fulfils the function of loss prevention but at the same time is an integral part of the business concept. Thus, it is important to expand the horizon of the research examining the nexus of surveillance and smart cities. In order to truly conceive a smart city concept that respects the privacy and the concerns of citizens, private companies and businesses must be included in any comprehensive strategy.

Lastly, due to limited funding and time, this thesis was only able to capture a snapshot of the debate surrounding the installation of new SOSTs, the practical implications for policing, and their social acceptability. It focused on surveillance as it is a core function of both smart cities and current crime prevention strategies in the UK. By doing so, however, it did not discuss other crime prevention initiatives in detail. Many more research topics aiming to explore either of these realms of the debate exist and will exist in the future as the discussion of this issue is only beginning. Amidst all these topics and all the future research that is to come, it is important not to forget the contribution that this thesis has provided to the academic field. As an author, I hope that this thesis does inspire further investigation of this interesting and important nexus and sparks new research ideas that provide valuable insights and shape policy developments in the UK and abroad.

It is difficult to predict how the use of smart SOSTs will develop in increasingly sophisticated and technology-driven urban environments when increasingly privacy and data protection concerns dominate the debate. It is safe to assume, however, that practitioners in London and the UK as a whole will have difficulty resisting the trend of increasing smartification also in the policing sector and that many debates and protests lie ahead. Accordingly, despite increasing public awareness and pressure of privacy rights and data protection, it can be assumed that the use of technology in everyday urban life will not decrease but rather steadily increase. For this reason, it is important not to work against the respective use of technology but to develop new ideas on how to use technologies responsibly and to create legal and ethical frameworks for their deployment.

REFERENCES

Abramovaite, J., Bandyopadhyay, S., Bhattacharya, S., & Cowen, N. (2018). Alternatives to custody: Evidence from police force areas in England and Wales. *The British Journal of Criminology, 59*(4), 800-822.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Adams, A., Baer, R., Denmon, S., & Dettmansperger, S. (2009). Glendale Police Department's strategic approach to staffing. *Alliance for Innovation Management Interns, October, 1*.

Adams, A. A., Arias-Oliva, M., Palma, A. M. L., & Murata, K. (2017a). Surveillance following Snowden: a major challenge in Spain. *Journal of Information, Communication and Ethics in Society*.

Adams, A. A., Hosell, S., & Murata, K. (2017b). Following Snowden, German uncertainty about monitoring. *Journal of Information, Communication and Ethics in Society*.

Adams, J., Hillier-Brown, F. C., Moore, H. J., Lake, A. A., Araujo-Soares, V., White, M., & Summerbell, C. (2016). Searching and synthesising 'grey literature'and 'grey information'in public health: critical reflections on three case studies. *Systematic reviews, 5*(1), 1-11.

Aden, H. (2019). Polizei und Technik zwischen Praxisanforderungen, Politik und Recht. *Vorgänge, 227* (3/2019), 7-20.

Adey, P. (2002). Secured and Sorted Mobilities: Examples from the Airport. *Surveillance & Society, 1*(4).

Agha, A., Ranjan, R., & Gan, W.-S. (2017). Noisy vehicle surveillance camera: A system to deter noisy vehicle in smart city. *Applied Acoustics, 117*, 236-245.

Ahir, S., Kapadia, S., Chauhan, J., & Sanghavi, N. (2018). *The Personal Stun-A Smart Device For Women's Safety.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., & Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities, 60*, 234-245.

Aichholzer, J. (2017). *Einführung in lineare Strukturgleichungsmodelle mit Stata* (1 ed.). Wiesbaden: Springer Fachmedien.

Akhras, G. (2000). Smart materials and smart systems for the future. *Canadian Military Journal, 1*(3), 25-31.

Akhter, F., Khadivizand, S., Lodyga, J., Siddiquei, H. R., Alahi, M. E. E., & Mukhopadhyay, S. (2019). *Design and development of an IoT enabled pedestrian counting and environmental monitoring system for a smart city.* Paper presented at the 2019 13th International Conference on Sensing Technology (ICST).

Al-Anbuky, A. (2014). *Sensor-actuator smart lighting system: system organizational concept and challenges.* Paper presented at the ICT for Sustainability 2014 (ICT4S-14).

Al-Muaythir, A., & Hossain, M. A. (2016). *Cloud-based parametrized publish/subscribe system for public safety applications in smarter cities.* Paper presented at the 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC).

Al-Shami, S., Zekri, A., El-Zaart, A., & Zantout, R. (2017). *On the parallelization of closed-set patterns classification for an automatic license plate recognition system.* Paper presented at the 2017 Sensors Networks Smart and Emerging Technologies (SENSET).

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., . . . Walker, S. (2012). *Building understanding of smart city initiatives.* Paper presented at the International conference on electronic government.

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

Alirol, E., Getaz, L., Stoll, B., Chappuis, F., & Loutan, L. (2011). Urbanisation and infectious diseases in a globalised world. *The Lancet infectious diseases, 11*(2), 131-141.

Allen, D., Wilson, T., Norman, A., & Knight, C. (2008). Information on the move: the use of mobile information systems by UK police forces. *Information Research, 13*(4), 13-14.

Almasawa, M. O., Elrefaei, L. A., & Moria, K. (2019). A survey on deep learning-based person re-identification systems. *IEEE Access, 7*, 175228-175247.

Aloi, G., Bedogni, L., Felice, M. D., Loscri, V., Molinaro, A., Natalizio, E., . . . Zema, N. R. (2014). STEM-Net: an evolutionary network architecture for smart and sustainable cities. *Transactions on Emerging Telecommunications Technologies, 25*(1), 21-40.

Altomare, A., & Cartlett, C. (2017). How Data Analysis Supports Crime Prediction in Smart Cities. *New Frontiers in High Performance Computing and Big Data, 30*, 215.

Ammicht Quinn, R., Koch, H., Held, C., Matzner, T., Krumm, J., Flack, J., . . . Wittmann, P. (2015). Intelligente Videoüberwachung: eine Handreichung.

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political geography, 25*(3), 336-351.

Anagnostopoulos, T. (2014). *A Surveillance System for Preventing Suicide Attempts in Urban Metro Stations.* Paper presented at the Proceedings of the 18th Panhellenic Conference on Informatics.

Anania, E. C., Rice, S., Pierce, M., Winter, S. R., Capps, J., Walters, N. W., & Milner, M. N. (2019). Public support for police drone missions depends on political affiliation and neighborhood demographics. *Technology in Society, 57*, 95-103.

Anderson, P., Chisholm, D., & Fuhr, D. C. (2009). Effectiveness and cost-effectiveness of policies and programmes to reduce the harm caused by alcohol. *The lancet, 373*(9682), 2234-2246.

Anees, V. M., & Kumar, G. S. (2017). *Direction estimation of crowd flow in surveillance videos.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Angel, S. (1968). *Discouraging crime through city planning.* Berkely, CA: University of California Institute of Urban & Regional Development.

Angiati, D., Gera, G., Piva, S., & Regazzoni, C. S. (2005). *A novel method for graffiti detection using change detection algorithm.* Paper presented at the IEEE Conference on Advanced Video and Signal Based Surveillance, 2005.

Ankitha, S., Nayana, K., Shravya, S., & Jain, L. (2017). *Smart city initiative: Traffic and waste management.* Paper presented at the Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on.

Anthopoulos, L. (2015). *Defining smart city architecture for sustainability.* Paper presented at the proceedings of 14th electronic government and 7th electronic participation conference (IFIP2015).

Apelt, M., & Möllers, N. (2011). Wie „intelligente "Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung. *Zeitschrift für Außen- und Sicherheitspolitik, 4*(4), 585-593.

Appleton, J. V. (1995). Analysing qualitative interview data: addressing issues of validity andreliability. *Journal of advanced nursing, 22*(5), 993-997.

Araujo, A., Cacho, N., Thome, A. C., Medeiros, A., & Borges, J. (2017). *A predictive policing application to support patrol planning in smart cities.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Arauz, M. R., Moreno, Y., Nancalres, R., Pérez, C. V., & Larios, V. M. (2017). *Tackling corruption in urban development through open data and citizen empowerment: The case of "visor urbano" in guadalajara.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Ariel, B. (2016). Increasing cooperation with the police using body worn cameras. *Police Quarterly, 19*(3), 326-362.

Armitage, R. (2002). To CCTV or not to CCTV. *A review of current research into the effectiveness of CCTV systems in reducing crime, 8*.

Armitage, R. (2013). The Impact of Surveillance on Levels of Crime and Fear of Crime. In R. Armitage (Ed.), *Crime Prevention through Housing Design* (pp. 144-152). London: Palgrave Macmillan.

Artyushina, A. (2020). Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. *Telematics and Informatics, 55*, 101456.

Ashby, M. P. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research, 23*(3), 441-459.

Ashby, M. P., & Bowers, K. J. (2013). A comparison of methods for temporal analysis of aoristic crime. *Crime Science, 2*(1), 1.

Austin, L., & Lie, D. (2021). Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust. *Surveillance & Society, 19*(2), 255-261.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Azoulay, P., & Jones, B. (2020). Beat COVID-19 through innovation (Vol. 368, pp. 553): American Association for the Advancement of Science.

Baba, M., Pescaru, D., Gui, V., & Jian, I. (2016). *Stray dogs behavior detection in urban area video surveillance streams.* Paper presented at the 2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC).

Babu, D. V., Nisha, A. S. A., Dhasan, D. B., Venkatesan, M., & Karthikeyan, C. (2021). Intelligent High Tech Street Lightning Pole for Smart City. *Annals of the Romanian Society for Cell Biology, 25*(4), 13752-13759.

Bachner, J. (2013). *Predictive policing: preventing crime with data and analytics.* Washington, DC: IBM Center for the Business of Government Washington, DC.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., . . . Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3-13.

Bakıcı, T., Almirall, E., & Wareham, J. (2013). A smart city initiative: the case of Barcelona. *Journal of the knowledge economy, 4*(2), 135-148.

Baldoni, G., Melita, M., Micalizzi, S., Rametta, C., Schembra, G., & Vassallo, A. (2017). *A dynamic, plug-and-play and efficient video surveillance platform for smart cities.* Paper presented at the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC).

Baldwin Jr, F. N., & Shaw, R. B. (2006). Down to the wire: Assessing the constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the rule of law. *U. Fla. JL & Pub. Pol'y, 17*, 429.

Balla, P. B., & Jadhao, K. (2018). *IoT Based Facial Recognition Security System.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Ballesteros, J., Rahman, M., Carbunar, B., & Rishe, N. (2012). *Safe cities. A participatory sensing approach.* Paper presented at the 37th Annual IEEE Conference on Local Computer Networks.

Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *J. Marshall J. Computer & Info. L., 18*, 1.

Bär, L., Ossewaarde, M., & van Gerven, M. (2020). The ideological justifications of the Smart City of Hamburg. *Cities, 105*, 102811.

Barba, C. T., Mateos, M. A., Soto, P. R., Mezher, A. M., & Igartua, M. A. (2012). *Smart city for VANETs using warning messages, traffic statistics and intelligent traffic lights.* Paper presented at the 2012 IEEE Intelligent Vehicles Symposium.

Barnes, C. Y., & Henly, J. R. (2018). "They are underpaid and understaffed": How clients interpret encounters with street-level bureaucrats. *Journal of Public Administration Research and Theory, 28*(2), 165-181.

Barrionuevo, J. M., Berrone, P., & Ricart, J. E. (2012). Smart cities, sustainable progress. *IESE Insight, 14*(14), 50-57.

Bartoli, G., Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2015). A novel emergency management platform for smart public safety. *International Journal of Communication Systems, 28*(5), 928-943.

Bartsch, S. (2011). *Practitioners' perspectives on security in agile development.* Paper presented at the 2011 Sixth International Conference on Availability, Reliability and Security.

Batty, M. (2013). Big data, smart cities and city planning. *Dialogues in Human Geography, 3*(3), 274-279.

Baumer, T. L. (1978). Research on fear of crime in the United States. *Victimology, 3*(3-4), 254-264.

Bayerl, P., & Butot, V. (2021). Smart City Configurations: A Conceptual Approach to Assess Smart City Practices and Outcomes.

Beamer, G. (2002). Elite interviews and state politics research. *State Politics & Policy Quarterly, 2*(1), 86-96.

Been, F., Esseiva, P., & Delémont, O. (2016). Analysis of illicit drugs in wastewater–Is there an added value for law enforcement? *Forensic science international, 266*, 215-221.

Beiter, R., Doria, J., Gottschaller, S., Kaeber, F., Kegel, J., & Leipold, C. (2020). Fühlt sich das noch gut an? Ein quantitativ-qualitatives Forschungsprojekt zur Akzeptanz der Künstlichen Intelligenz im Alltag.

Belbachir, A. N. (2010). *Smart cameras* (Vol. 2). New York: Springer.

Bellini, P., Cenni, D., Nesi, P., & Paoli, I. (2017). Wi-Fi based city users' behaviour analysis for smart city. *Journal of Visual Languages & Computing, 42*, 31-45.

Belur, J., Tompson, L., Thornton, A., & Simon, M. (2018). Interrater reliability in systematic review methodology: exploring variation in coder decision-making. *Sociological methods & research*, 0049124118799372.

Beniger, J. (2009). *The control revolution: Technological and economic origins of the information society*. Cambridge, MA: Harvard University Press.

Benjamin, C. (2002). Shot spotter and faceit: The tools of mass monitoring. *UCLA Journal of Law and Technology, 6*, 1-24.

Benkő, M., & Germán, T. (2016). Crime prevention aspects of public space renewal in Budapest. *Journal of Place Management and Development, 9*(2), 191-209.

Bennett, C. J. (1995). The political economy of privacy: a review of the literature. *Hackensack, NJ: Center for Social and Legal Research.*

Bennett, C. J. (2015). Trends in voter surveillance in Western societies: privacy intrusions and democratic implications.

Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society, 28*(7), 806-822.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological bulletin, 107*(2), 238.

Bentler, P. M. (1995). *EQS structural equations program manual* (Vol. 6). Encino, CA: Multivariate software.

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy, 1*(2), 243-264.

Berry, B. J. (2015). *The human consequences of urbanisation* (Vol. 1). London: Macmillan International Higher Education.

Berry, M. (2018). Technology and organised crime in the smart city: an ethnographic study of the illicit drug trade. *City, Territory and Architecture, 5*(1), 16.

Best, S. J., & Krueger, B. S. (2011). Government monitoring and political participation in the United States: The distinct roles of anger and anxiety. *American Politics Research, 39*(1), 85-117.

Beste, H. (2000). Neue Sicherheit für die Stadt. *Neue Kriminalpolitik*, 17-21.

Bettencourt, L. M. (2014). The uses of big data in cities. *Big Data, 2*(1), 12-22.

Beyers, J., Braun, C., Marshall, D., & De Bruycker, I. (2014). Let's talk! On the practice and method of interviewing policy experts. *Interest Groups & Advocacy, 3*(2), 174-187.

Bieber, C. (2018). Smart City "und „Civic Tech *Die mediatisierte Stadt* (pp. 177-194). Wiesbaden: Springer.

Bier, C. (2012). Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz? *Computer und Recht, 28*(9), 610-618.

Bifulco, F., Tregua, M., Amitrano, C. C., & D'Auria, A. (2016). ICT and sustainability in smart cities management. *International Journal of Public Sector Management, 29*(2), 132-147.

Bomfim, R. A., de Souza, L. B., & Corrente, J. E. (2018). Tooth loss and its relationship with protein intake by elderly Brazilians—a structural equation modelling approach. *Gerodontology, 35*(1), 51-58.

Bonatsos, A., Middleton, L., Melas, P., & Sabeur, Z. (2013). *Crime open data aggregation and management for the design of safer spaces in urban environments.* Paper presented at the International Symposium on Environmental Software Systems.

Boon, L. S., Malek, J. A., Hussain, M., & Tahir, Z. (2017). *Citizen participation in realising the citizen-centric vision for smart city.* Paper presented at the Social, Environmental and Developmental Sustainability Research Centre International Conference.

Borges, J., Ziehr, D., Beigl, M., Cacho, N., Martins, A., Sudrich, S., . . . Etter, M. (2017). *Feature engineering for crime hotspot detection.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Borins, S. (2002). Leadership and innovation in the public sector. *Leadership & Organization Development Journal, 23*(8), 467-476. doi:10.1108/01437730210449357

Bornewasser, M., & Kober, M. (2012). *Videoüberwachung: Kriminalitätsreduzierung und gezielte Verdrängung. Bericht über eine Evaluationsmaßnahme in der Stadt Luxemburg.* Paper presented at the Forum Kriminalprävention.

Bornewasser, M., & Schulz, F. (2008). Ergebnisse der Evaluationsstudie im Land Brandenburg. *Bornewasser, Manfred (Hg.): Videoüberwachung öffentlicher Straßen und Plätze, Ergebnisse eines Pilotprojektes in Brandenburg. Frankfurt.*

Borrion, H. (2018). Engineering. In R. Wortley, A. Sidebottom, N. Tilley, & G. Laycock (Eds.), *Routledge Handbook of Crime Science* (pp. 167-178): Routledge.

Borrion, H., Ekblom, P., Alrajeh, D., Borrion, A. L., Keane, A., Koch, D., . . . Toubaline, S. (2019). The Problem with Crime Problem-Solving: Towards a Second Generation Pop? *The British Journal of Criminology.*

Borrion, H., Kurland, J., Tilley, N., & Chen, P. (2020). Measuring the resilience of criminogenic ecosystems to global disruption: A case-study of COVID-19 in China. *Plos one, 15*(10), e0240077.

Borrion, H., Tripathi, K., Chen, P., & Moon, S. (2014). Threat detection: A framework for security architects and designers of metropolitan rail systems. *Urban, Planning and Transport Research, 2*(1), 173-194.

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). *Towards understanding IT security professionals and their tools.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

Boukerche, A., Siddiqui, A. J., & Mammeri, A. (2017). Automated Vehicle Detection and Classification: Models, Methods, and Techniques. *ACM Computing Surveys (CSUR), 50*(5), 62.

Boulton, L., McManus, M., Metcalfe, L., Brian, D., & Dawson, I. (2017). Calls for police service: Understanding the demand profile and the UK police response. *The Police Journal, 90*(1), 70-85.

Bourmpos, M., Argyris, A., & Syvridis, D. (2014). Smart city surveillance through low-cost fiber sensors in metropolitan optical networks. *Fiber and Integrated Optics, 33*(3), 205-223.

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and society magazine, 23*(1), 9-19.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks, CA: Sage.

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. *The British Journal of Criminology, 60*(6), 1502-1522. doi:10.1093/bjc/azaa032

Braga, A. A. (2016). The continued importance of measuring potentially harmful impacts of crime prevention programs: The academy of experimental criminology 2014 Joan McCord lecture. *Journal of experimental criminology, 12*(1), 1-20.

Braga, A. A., & Weisburd, D. (2006). Police innovation and the future of policing. *Police innovation: Contrasting perspectives*, 339-352.

Bramley, G., Brown, C., Dempsey, N., Power, S., & Watkins, D. (2010). Social acceptability *Dimensions of the sustainable city* (pp. 105-128): Springer.

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review, 4*(5), 193-220.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

Brandl, S. G., Frank, J., Worden, R. E., & Bynum, T. S. (1994). Global and specific attitudes toward the police: Disentangling the relationship. *Justice quarterly, 11*(1), 119-134.

Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. *Statistics and Public Policy, 5*(1), 1-6.

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable cities and society, 39*, 499-507.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977-1008.

Brell, T., Philipsen, R., & Ziefle, M. (2018). Pictures of You, Pictures of Me.

Breuil, B. O., Schuilenburg, M., & van Steden, R. (2014). *Positive criminology: reflections on care, belonging and security*. The Hague: Eleven International Publishing.

Brezeale, D., & Cook, D. J. (2008). Automatic video classification: A survey of the literature. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38*(3), 416-430.

Bromberg, D. E., Charbonneau, É., & Smith, A. (2019). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, 101415.

Brookman, F., & Jones, H. (2021). Capturing killers: the construction of CCTV evidence during homicide investigations. *Policing and Society*, 1-20.

Brown, D. (2020). Criminal justice in an age of austerity: The London Bridge killings. *Alternative Law Journal, 45*(4), 238-246.

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of internet surveillance. *European Journal of Criminology, 6*(2), 119-134.

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*. New York: Guilford publications.

Brownell Jr, H. (1953). Public Security and Wire Tapping. *Cornell LQ, 39*, 195.

Brust, M. R., Danoy, G., Bouvry, P., Gashi, D., Pathak, H., & Gonçalves, M. P. (2017). *Defending against intrusion of malicious uavs with networked uav defense swarms*. Paper presented at the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops).

Bryman, A., & Cassell, C. (2006). The researcher interview: a reflexive perspective. *Qualitative Research in Organizations and Management: an international journal, 1*(1), 41-55. doi:https://doi.org/10.1108/17465640610666633

Büllesfeld, D. (2002). *Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsvorsorge*. Stuttgart: Boorberg.

Bulut, E., Clément, C., Dura, G., Fischer, S., Franke, B., Gowan, R., . . . Ioannides, I. (2009). *European Security and Defence Policy: the first ten years (1999-2009)*. Brussels: The European Union Institute for Security Studies.

Burnay, M. (2019). *Privacy and Surveillance in a Digital Era: Transnational Implications of China's Surveillance State*. Retrieved from

Butler, G. (2005). Shoplifters views on security: Lessons for crime prevention *Crime At Work* (pp. 56-72): Springer.

Byon, S., Kwon, E., Jung, E.-S., & Lee, Y.-T. (2017). *A study on location information aided re-identification in CCTV environment*. Paper presented at the 2017 International Conference on Information and Communication Technology Convergence (ICTC).

Byun, J.-Y., Nasridinov, A., & Park, Y.-H. (2014). Internet of things for smart crime detection. *Contemporary Engineering Sciences, 7*(15), 749-754.

Cagliero, L., Cerquitelli, T., Chiusano, S., Garino, P., Nardone, M., Pralio, B., & Venturini, L. (2015). *Monitoring the citizens' perception on urban security in Smart City environments.* Paper presented at the 2015 31st IEEE International Conference on Data Engineering Workshops.

Calavia, L., Baladrón, C., Aguiar, J. M., Carro, B., & Sánchez-Esguevillas, A. (2012). A semantic autonomous video surveillance system for dense camera networks in smart cities. *Sensors, 12*(8), 10407-10429.

Camboim, H. B., Neto, A. J. V., Rodrigues, J. J., & Zhao, Z. (2017). *Applying Fog Computing to Improve Crime Assistance in Smart Transportation Safety Systems.* Paper presented at the 2017 IEEE First Summer School on Smart Cities (S3C).

Cameron, A., Kolodinski, E., May, H., & Williams, N. (2008). Measuring the effects of video surveillance on crime in Los Angeles. *Report prepared for the California Research Bureau. USC School of Policy, Planning, and Development.*

Campbell, J. E., & Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586-606.

Campbell, J. H., Brann, J., & Williams, D. (2003). Officer-Per-Thousand Formulas & Other Policing Myths: A Leadership Model for Better Police Resource Management. *Portland, OR: Campbell DeLong Resources.*

Cannataci, J. A. (2010). *Squaring the circle of smart surveillance and privacy.* Paper presented at the 2010 Fourth International Conference on Digital Society.

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

Capers, I. B. (2016). Race, Policing, and Technology. *NCL Rev., 95*, 1241.

Caplan, J. M., Kennedy, L. W., & Petrossian, G. (2011). Police-monitored CCTV cameras in Newark, NJ: A quasi-experimental test of crime deterrence. *Journal of experimental criminology, 7*(3), 255-274.

Caragliu, A., & Del Bo, C. F. (2018). Smart innovative cities: The impact of Smart City policies on urban innovation. *Technological Forecasting and Social Change.*

Cardullo, P., & Kitchin, R. (2019). Being a 'citizen'in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. *GeoJournal, 84*(1), 1-13.

Carr, C., & Hesse, M. (2020). Sidewalk Labs closed down–whither Google's smart city? *Regions-E-Magazine*(7).

Carr, J., & Doleac, J. L. (2016). The geography, incidence, and underreporting of gun violence: new evidence using ShotSpotter data. *Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data (April 26, 2016).*

Carreño, P., Gutierrez, F. J., Ochoa, S. F., & Fortino, G. (2015). Supporting personal security using participatory sensing. *Concurrency and Computation: Practice and Experience, 27*(10), 2531-2546.

Carter, S. P., Carter, S. L., & Dannenberg, A. L. (2003). Zoning out crime and improving community health in Sarasota, Florida:"crime prevention through environmental design". *American Journal of Public Health, 93*(9), 1442-1445.

Castella-Roca, J., Mut-Puigserver, M., Payeras-Capella, M. M., Viejo, A., & Angles-Tafalla, C. (2017). *Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas.* Paper presented at the 2017 26th International Conference on Computer Communication and Networks (ICCCN).

Castelli, M., Sormani, R., Trujillo, L., & Popovič, A. (2017). Predicting per capita violent crimes in urban areas: an artificial intelligence approach. *Journal of Ambient Intelligence and Humanized Computing, 8*(1), 29-36.

Castelnovo, W., Misuraca, G., & Savoldelli, A. (2016). Smart cities governance: The need for a holistic approach to assessing urban participatory policy making. *Social science computer review, 34*(6), 724-739.

Catlett, C., Cesario, E., Talia, D., & Vinci, A. (2018). *A Data-Driven Approach for Spatio-Temporal Crime Predictions in Smart Cities.* Paper presented at the 2018 IEEE International Conference on Smart Computing (SMARTCOMP).

Catlett, C., Cesario, E., Talia, D., & Vinci, A. (2019). Spatio-temporal crime predictions in smart cities: A data-driven approach and experiments. *Pervasive and Mobile Computing.*

Cavoukian, A. (2009a). Privacy by design.

Cavoukian, A. (2009b). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada, 5*, 12.

Ceccato, V. (2020a). The architecture of crime and fear of crime: Research evidence on lighting, CCTV and CPTED features 1 *Crime and fear in public places* (pp. 38-72): Routledge.

Ceccato, V. (2020b). Research evidence on lighting, CCTV and CPTED features1. *Crime and Fear in Public Places: Towards Safe, Inclusive and Sustainable Cities*, 38.

Cécile, M., & Born, M. (2009). Intervention in juvenile delinquency: Danger of iatrogenic effects? *Children and Youth Services Review, 31*(12), 1217-1221.

Cemgil, T., Kurutmaz, B., Cezayirli, A., Bingol, E., & Sener, S. (2017). *Interpolation and fraud detection on data collected by automatic meter reading.* Paper presented at the 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG).

Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. *European Journal of Criminology, 10*(2), 222-236.

Chackravarthy, S., Schmitt, S., & Yang, L. (2018). *Intelligent Crime Anomaly Detection in Smart Cities Using Deep Learning.* Paper presented at the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).

Chan, J. (2003). Police and new technologies. *Handbook of Policing*, 655-679.

Chan, J. B. (2001). The technological game: How information technology is transforming police practice. *Criminal justice, 1*(2), 139-159.

Chen, N., Chen, Y., You, Y., Ling, H., Liang, P., & Zimmermann, R. (2016). *Dynamic urban surveillance video stream processing using fog computing.* Paper presented at the 2016 IEEE second international conference on multimedia big data (BigMM).

Chen, X., Xu, J.-B., & Guo, W.-Q. (2013). *The research about video surveillance platform based on cloud computing.* Paper presented at the 2013 International Conference on Machine Learning and Cybernetics.

Chen, Z., Fan, W., Xiong, Z., Zhang, P., & Luo, L. (2010). Visual data security and management for smart cities. *Frontiers of Computer Science in China, 4*(3), 386-393.

Cheurprakobkit, S. (2000). Police-citizen contact and police performance attitudinal differences between Hispanics and non-Hispanics. *Journal of Criminal Justice, 28*(4), 325-336.

Chiodi, S. I. (2016). Crime prevention through urban design and planning in the smart city era: The challenge of disseminating CP-UDP in Italy: learning from Europe. *Journal of Place Management and Development, 9*(2), 137-152.

Chmutina, K., & Bosher, L. (2017). Rapid Urbanisation and Security: Holistic Approach to Enhancing Security of Urban Spaces *The Palgrave Handbook of Security, Risk and Intelligence* (pp. 27-45): Springer.

Cho, Y. I. (2012). *Designing smart cities: Security issues.* Paper presented at the IFIP International Conference on Computer Information Systems and Industrial Management.

Choi, W., & Na, J. (2017). *Relative importance for crime prevention technologies as part of smart city based on spatial information.* Paper presented at the 2017 Smart City Symposium Prague.

Chong, H. G. (2008). Measuring performance of small-and-medium sized enterprises: The grounded theory approach. *Journal of Business & Public Affairs, 2*(1), 1-11.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., . . . Scholl, H. J. (2012). *Understanding smart cities: An integrative framework.* Paper presented at the 2012 45th Hawaii international conference on system sciences.

Christopoulos, D. (2009). *Peer Esteem Snowballing: A methodology for expert surveys.* Paper presented at the Eurostat conference for new techniques and technologies for statistics.

Clare, J., Henstock, D., McComb, C., Newland, R., Barnes, G. C., Lee, M., & Taylor, E. (2019). Police, public, and arrestee perceptions of body-worn video: A single jurisdictional multiple-perspective analysis. *Criminal justice review, 44*(3), 304-321.

Clarke, R. (1997). Situational crime prevention (pp. 53–70). *Monsey, NY: Criminal.*

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91-150.

Clothier, R. A., Greer, D. A., Greer, D. G., & Mehta, A. M. (2015). Risk perception and the public acceptance of drones. *Risk analysis, 35*(6), 1167-1183.

Cocchia, A. (2014). Smart and digital city: A systematic literature review *Smart city* (pp. 13-43): Springer.

Coe, A., Paquet, G., & Roy, J. (2001). E-governance and smart communities: a social learning challenge. *Social science computer review, 19*(1), 80-93.

Cohen, I. G., & Mello, M. M. (2019). Big data, big tech, and protecting patient privacy. *Jama, 322*(12), 1141-1142.

Coleman, R. (2012). *Reclaiming the streets.* Liverpool: Routledge.

Coleman, R., & McCahill, M. (2010). *Surveillance and crime.* Thousand Oaks, CA: Sage.

College of Policing. (2021). CCTV. *Crime Recuction Toolkit* Retrieved from https://whatworks.college.police.uk/toolkit/Pages/Intervention.aspx?InterventionID=1

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies, 16*, 41-96.

Côté-Boucher, K. (2008). The diffuse border: intelligence-sharing, control and confinement along Canada's smart border. *Surveillance & Society, 5*(2), 142-165.

Cozens, P. (2007). Planning, crime and urban sustainability. *WIT Transactions on Ecology and the Environment, 102*.

Cozens, P., & Davies, T. (2013). Crime and residential security shutters in an Australian suburb: Exploring perceptions of 'Eyes on the Street', social interaction and personal safety. *Crime prevention and community safety, 15*(3), 175-191.

Cozens, P. M. (2002). Sustainable urban development and crime prevention through environmental design for the British city. Towards an effective urban environmentalism for the 21st century. *Cities, 19*(2), 129-137.

Cozens, P. M., Saville, G., & Hillier, D. (2005). Crime prevention through environmental design (CPTED): a review and modern bibliography. *Property management, 23*(5), 328-356.

Cretu, L.-G. (2012). Smart cities design using event-driven paradigm and semantic web. *Informatica Economica, 16*(4), 57.

Crow, M. S., & Smykla, J. O. (2019). Police body-worn cameras: Research developments on an emerging technology. *44*(3), 257-262. doi:https://doi.org/10.1177/0734016819854789

Crowe, T. (2000). *Crime prevention through environmental design*. London: Butterworth-Heinemann.

Cubik, J., Kepak, S., Nedoma, J., Fajkus, M., Zboril, O., Novak, M., . . . Vasinek, V. (2017). *Fiber optic perimeter system for security in smart city*. Paper presented at the Electro-Optical Remote Sensing XI.

Cuevas, Q. D. P., Corachea, J. C. P., Escabel, E. B., & Bautista, M. L. A. (2016). Effectiveness of CCTV Cameras Installation In Crime Prevention.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science, 10*(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues, 59*(2), 323-342.

Curran, D., & Smart, A. (2021). Data-driven governance, smart urbanism and risk-class inequalities: Security and social credit in China. *Urban Studies, 58*(3), 487-506.

Custers, B., & Vergouw, B. (2015). Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies. *Computer Law & Security Review, 31*(4), 518-526.

Cvrtila, V., & Perešin, A. (2014). New security models and public-private partnership. *Collegium antropologicum, 38*(1), 195-204.

Dai, M., Hu, X., & Gu, F. (2020). Citizen Characteristics, Neighbourhood Conditions, and Prior Contacts with the Police: A Comparative Study of Public Satisfaction with the Police. *Canadian Journal of Criminology and Criminal Justice, 62*(4), 77-101.

Dai, M., Hu, X., & Time, V. (2019). Understanding public satisfaction with the police. *Policing: An International Journal.*

Dai, M., & Jiang, X. (2016). A comparative study of satisfaction with the police in the United States and Australia. *Australian & New Zealand Journal of Criminology, 49*(1), 30-52.

Dai, M., & Johnson, R. R. (2009). Is neighborhood context a confounder? *Policing: An International Journal of Police Strategies & Management.*

Dameri, R. P. (2013). Searching for smart city definition: a comprehensive proposal. *international Journal of computers & technology, 11*(5), 2544-2551.

Dameri, R. P., Negre, E., & Rosenthal-Sabroux, C. (2016). *Triple Helix in Smart cities: a literature review about the vision of public bodies, universities, and private companies.* Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Danzer, A., Feuerbaum, C., & Gaessler, F. (2020). Labor supply and automation innovation. *Max Planck Institute for Innovation & Competition Research Paper*(20-09).

Datta, S., & Sarkar, S. (2017). *Automation, security and surveillance for a smart city: Smart, digital city.* Paper presented at the 2017 IEEE Calcutta Conference (CALCON).

Davies, T., & Bowers, K. (2019). Patterns in the supply and demand of urban policing at the street segment level. *Policing and Society, 30*(7), 795-817. doi:https://doi.org/10.1080/10439463.2019.1598997

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28-46.

Davoudi, S. (2014). Climate change, securitisation of nature, and resilient urbanism. *Environment and Planning C: Government and Policy, 32*(2), 360-375.

Dbouk, M., Mcheick, H., & Sbeity, I. (2014). CityPro; An integrated city-protection collaborative platform. *Procedia Computer Science, 37*, 72-79.

de Diego, I. M., San Román, I., Montero, J. C., Conde, C., & Cabello, E. (2018). Scalable and flexible wireless distributed architecture for intelligent video surveillance systems. *Multimedia Tools and Applications, 78*, 17437-17459. doi:https://doi.org/10.1007/s11042-018-7065-3

de Kort, Y., IJsselsteijn, W., Haans, A., Lakens, D., Kalinauskaite, I., & Schietecat, A. (2014). *De-escalate: Defusing escalating behaviour through the use of interactive light scenarios.* Paper presented at the Proc. Experiencing Light.

Deakin, M. (2014). Smart cities: the state-of-the-art and governance challenge. *Triple Helix, 1*(1), 7.

Debnath, A. K., Chin, H. C., Haque, M. M., & Yuen, B. (2014). A methodological framework for benchmarking smart transport cities. *Cities, 37*, 47-56.

Degeling, M. (2014). „Profiling, Prediction und Privatheit: Über das Verhältnis eines liberalen Privatheitbegriffs zu neueren Techniken der Verhaltensvorhersage ". *Medien und Privatheit, Medien, Texte, Semiotik*, 69-92.

Degeling, M., & Berendt, B. (2017). What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *AI & SOCIETY*, 1-10.

Denemark, D. (2012). Trust, efficacy and opposition to anti-terrorism police power: Australia in comparative perspective. *Australian Journal of Political Science, 47*(1), 91-113.

Desai, G., Ambre, V., Jakharia, S., & Sherkhane, S. (2018). *Smart Road Surveillance Using Image Processing.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Desoi, M. (2018). *Intelligente Videoüberwachung: Rechtliche Bewertung und rechtsgemäße Gestaltung.* Berlin: Springer.

Dey, S., Chakraborty, A., Naskar, S., & Misra, P. (2012). *Smart city surveillance: Leveraging benefits of cloud data stores.* Paper presented at the 37th Annual IEEE Conference on Local Computer Networks-Workshops.

Di Leo, G., & Sardanelli, F. (2020). Statistical significance: p value, 0.05 threshold, and applications to radiomics—reasons for a conservative approach. *European radiology experimental, 4*(1), 1-8.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology, 45*(3), 285-297.

Dilshad, N., Hwang, J., Song, J., & Sung, N. (2020). *Applications and Challenges in Video Surveillance via Drone: A Brief Survey.* Paper presented at the 2020 International Conference on Information and Communication Technology Convergence (ICTC).

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management (JGIM), 14*(4), 57-93.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233.

Dishion, T. J., McCord, J., & Poulin, F. (1999). When interventions harm: Peer groups and problem behavior. *American psychologist, 54*(9), 755.

Ditton, J. (2000). Crime and the city. *British Journal of Criminology, 40*(4), 692-709.

Ditton, J., & Short, E. (1998). When open street CCTV appears to reduce crime: does it just get displaced elsewhere. *CCTV Today, 5*(2), 13-16.

Ditton, J., Short, E., Phillips, S., Norris, C., & Armstrong, G. (1999). *The effect of closed circuit television on recorded crime rates and public concern about crime in Glasgow.* Glasgow: CRU.

Dix, A. (2016). Datenschutz im Zeitalter von Big Data: wie steht es um den Schutz der Privatsphäre? *Stadtforschung und Statistik: Zeitschrift des Verbandes Deutscher Städtestatistiker, 29*(1), 59-64.

Dixon, J., Levine, M., & McAuley, R. (2004). Street drinking legislation, CCTV and public space: Exploring attitudes towards public order measures. *Online Report for Home Office.*

Dizon, E., & Pranggono, B. (2021). Smart streetlights in Smart City: a case study of Sheffield. *Journal of Ambient Intelligence and Humanized Computing*, 1-16.

Dorussen, H., Lenz, H., & Blavoukos, S. (2005). Assessing the reliability and validity of expert interviews. *European Union Politics, 6*(3), 315-337.

Du Plessis, C. (1999). The links between crime prevention and sustainable development. *Open house international, 24*, 33-40.

Duan, L., Lou, Y., Wang, S., Gao, W., & Rui, Y. (2018). AI oriented large-scale video management for smart city: Technologies, standards and beyond. *IEEE MultiMedia*.

Duff, R. A., & Marshall, S. E. (2000). Benefits, Burdens and Responsibilities: Some Ethical Dimensions of Situational Crime Prevention. In A. Von Hirsch, D. Garland, & A. Wakefield (Eds.), *Ethical and social perspectives on situational crime prevention* (Vol. 1): Hart Publishing.

Duque, D., Santos, H., & Cortez, P. (2007). *Prediction of abnormal behaviors for intelligent video surveillance systems.* Paper presented at the 2007 IEEE Symposium on Computational Intelligence and Data Mining.

Durga, S., Surya, S., & Daniel, E. (2018). *SmartMobiCam: Towards a New Paradigm for Leveraging Smartphone Cameras and IaaS Cloud for Smart City Video Surveillance.* Paper presented at the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).

Durlauf, S. N., & Heckman, J. J. (2020). An Empirical Analysis of Racial Differences in Police Use of Force: A Comment. *Journal of Political Economy, 128*(10), 3998-4002.

Dutton, W., Guerra, G. A., Zizzo, D. J., & Peltu, M. (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity, 10*(1, 2), 13-23.

Edwards, L. (2005). Switching off the surveillance society? Legal regulation of CCTV in the UK.

Eger, J. M. (2009). Smart growth, smart cities, and the crisis at the pump a worldwide phenomenon. *I-WAYS-The Journal of E-Government Policy and Regulation, 32*(1), 47-53.

Egnoto, M., Ackerman, G., Iles, I., Roberts, H. A., Smith, D. S., Liu, B. F., & Behlendorf, B. (2017). What motivates the blue line for technology adoption? Insights from a police expert panel and survey. *Policing: An International Journal of Police Strategies & Management.*

Eigenmann, P., & Rieger-Ladich, M. (2010). Michel Foucault: Überwachen und Strafen. Die Geburt des Gefängnisses *Schlüsselwerke der Identitätsforschung* (pp. 223-239): Springer.

Eigenraam, D., & Rothkrantz, L. (2016). *A smart surveillance system of distributed smart multi cameras modelled as agents.* Paper presented at the 2016 Smart Cities Symposium Prague (SCSP).

Ekblom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on crime and crime prevention, 8*, 27-51.

Ekblom, P. (2001). Future imperfect: Preparing for the crimes to come.

Ekblom, P. (2005). How to police the future: Scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction. In M. J. Smith & N. Tilley (Eds.), *Crime Science - New Approaches to Preventing and Detecting Crime*. Devon: Willian Publishing.

Ekblom, P. (2017). Technology, opportunity, crime and crime prevention: current and evolutionary perspectives *Crime Prevention in the 21st Century* (pp. 319-343): Springer.

Ekblom, P., & Hirschfield, A. (2014). Developing an alternative formulation of SCP principles–the Ds (11 and counting). *Crime Science, 3*(1), 2.

Elliott-Davies, M., Donnelly, J., Boag-Munroe, F., & Van Mechelen, D. (2016). 'Getting a battering' The perceived impact of demand and capacity imbalance within the Police Service of England and Wales: A qualitative review. *The Police Journal, 89*(2), 93-116.

Ellison, G. T. (2005). 'Population profiling'and public health risk: when and how should we use race/ethnicity?

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491-497.

Erickson, B. H. (1979). Some problems of inference from chain data. *Sociological methodology, 10*, 276-302.

Ertugrul, E., Kocaman, U., & Sahingoz, O. K. (2018). *Autonomous aerial navigation and mapping for security of smart buildings*. Paper presented at the 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG).

Etzioni, A. (2005). The limits of privacy. *Contemporary Debates in Applied Ethics. Oxford: Blackwell*, 253-262.

Etzkowitz, H., & Zhou, C. (2006). Triple Helix twins: innovation and sustainability. *Science and public policy, 33*(1), 77-83.

Eugene III, A. (2001). *Rethinking police culture: Officers' occupational attitudes*. Retrieved from El Paso, TX:

Faller, I., & Scheiner, J. (2020). Wo lebt es sich am sichersten? Strukturgleichungsmodell des Verkehrsunfallrisikos in Niedersachen. *Stadtforschung und Statistik: Zeitschrift des Verbandes Deutscher Städtestatistiker, 33*(2), 9-14.

Fan, M. D. (2016). Justice visualized: Courts and the body camera revolution. *UCDL Rev., 50*, 897.

Fan, M. D. (2017). Democratizing proof: Pooling public and police body-camera videos. *NCL Rev., 96*, 1639.

Farrington, D. P., Gill, M., Waples, S. J., & Argomaniz, J. (2007). The effects of closed-circuit television on crime: Meta-analysis of an English national quasi-experimental multi-site evaluation. *Journal of experimental criminology, 3*(1), 21-38.

Fay, S. J. (1998). Tough on crime, tough on civil liberties: some negative aspects of Britain's wholesale adoption of CCTV surveillance during the 1990s. *International review of law, computers & technology, 12*(2), 315-347.

Federici, J. F., Schulkin, B., Huang, F., Gary, D., Barat, R., Oliveira, F., & Zimdars, D. (2005). THz imaging and sensing for security applications—explosives, weapons and drugs. *Semiconductor Science and Technology, 20*(7), S266.

Felson, M., & Clarke, R. V. (2016). The ethics of situational crime prevention *Rational choice and situational crime prevention: Theoretical foundations* (pp. 197-218): Taylor and Francis Inc.

Feng, G. C. (2014). Intercoder reliability indices: disuse, misuse, and abuse. *Quality & Quantity, 48*(3), 1803-1815.

Ferguson, A. G. (2014). Big data and predictive reasonable suspicion. *U. Pa. L. Rev., 163*, 327.

Ferguson, A. G. (2019). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: NYU Press.

Fernández, J., Calavia, L., Baladrón, C., Aguiar, J., Carro, B., Sánchez-Esguevillas, A., . . . Smilansky, Z. (2013). An intelligent surveillance platform for large metropolitan areas with dense sensor deployment. *Sensors, 13*(6), 7414-7442.

Fernandez-Anez, V., Fernández-Güell, J. M., & Giffinger, R. (2018). Smart City implementation and discourses: An integrated conceptual model. The case of Vienna. *Cities, 78*, 4-16.

Fernández-Güell, J.-M., Collado-Lara, M., Guzmán-Araña, S., & Fernández-Añez, V. (2016). Incorporating a systemic and foresight approach into smart city initiatives: the case of Spanish cities. *Journal of Urban Technology, 23*(3), 43-67.

Ferreira, J. E., Visintin, J. A., Okamoto, J., & Pu, C. (2017). *Smart services: A case study on smarter public safety by a mobile app for University of São Paulo.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Filipponi, L., Vitaletti, A., Landi, G., Memeo, V., Laura, G., & Pucci, P. (2010). *Smart city: An event driven architecture for monitoring public spaces with heterogeneous sensors.* Paper presented at the 2010 Fourth International Conference on Sensor Technologies and Applications.

Foucault, M. (1975). Discipline and punish. *A. Sheridan, Tr., Paris, FR, Gallimard.*

Fox, N. J. (1998). Foucault, Foucauldians and sociology. *British Journal of Sociology*, 415-433.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security, 2020*(12), 6-12.

Furnham, A., & Swami, V. (2019). Attitudes toward Surveillance: Personality, Belief and Value Correlates. *Psychology, 10*(5), 609-623.

Fussey, P. (2007). Observing potentiality in the global city: Surveillance and counterterrorism in London. *International Criminal Justice Review, 17*(3), 171-192.

Fussey, P., & Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology.

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology, 30*(1), 9-37.

García, C. G., Meana-Llorián, D., G-Bustelo, B. C. P., Lovelle, J. M. C., & Garcia-Fernandez, N. (2017). Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes. *Future Generation Computer Systems, 76*, 301-313.

García Fernández, C., & Peek, D. (2020). Smart and sustainable? Positioning adaptation to climate change in the European smart city. *Smart Cities, 3*(2), 511-526.

García, R. O., Valentín, L., Serrano, S. A., Palacios-Alonso, M. A., & Sucar, L. E. (2017). GEOVISUALIZATION FOR SMART VIDEO SURVEILLANCE. *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences, 4*.

Garg, R., Malik, A., & Raj, G. (2018). *A Comprehensive Analysis for Crime Prediction in Smart City Using R Programming.* Paper presented at the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

Garicano, L., & Heaton, P. (2010). Information technology, organization, and productivity in the public sector: Evidence from police departments. *Journal of Labor Economics, 28*(1), 167-201.

Garland, D. (2008). *Kultur der Kontrolle: Verbrechensbekämpfung und soziale Ordnung in der Gegenwart.* Frankfurt: Campus-Verlag.

Gärling, T., Jakobsson, C., Loukopoulos, P., & Fujii, S. (2008). Acceptability of road pricing. In E. T. Verhoef, M. C. J. Bliemer, L. Steg, & B. van Wee (Eds.), *Pricing in road transport: A multi-disciplinary perspective* (pp. 193). Cheltenham, UK/Northampton, MA, USA: Edward Elgar.

Garvie, C., & Frankle, J. (2016). Facial-recognition software might have a racial bias problem. *The Atlantic, 7*.

Gatti, U., Tremblay, R. E., & Vitaro, F. (2009). Iatrogenic effect of juvenile justice. *Journal of Child Psychology and Psychiatry, 50*(8), 991-998.

Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science, 52*, 1089-1094.

Gecas, A. S. (2016). Gunfire Game Changer or Big Brother's Hidden Ears: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology. *U. Ill. L. Rev.*, 1073.

Gerell, M. (2016). Hot spot policing with actively monitored CCTV cameras: Does it reduce assaults in public places? *International Criminal Justice Review, 26*(2), 187-201.

Germain, S., Douillet, A.-C., & Dumoulin, L. (2011). The legitimization of CCTV as a policy tool: Genesis and stabilization of a socio-technical device in three French cities. *The British Journal of Criminology, 52*(2), 294-308.

Gerrard, G., & Thompson, R. (2011). Two million cameras in the UK. *CCTV image, 42*(10), 9-12.

Giddens, A. (1985). Nation-state and violence: Polity Press.

Giffinger, R., Fertner, C., Kramar, H., & Meijers, E. (2007). City-ranking of European medium-sized cities. *Cent. Reg. Sci. Vienna UT*, 1-12.

Giffinger, R., & Haindlmaier, G. (2010). Smart cities ranking: an effective instrument for the positioning of the cities? *ACE: architecture, city and environment, 4*(12), 7-26.

Gil-Garcia, J. R., Pardo, T. A., & Nam, T. (2015). What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Information Polity, 20*(1), 61-87.

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV* (Vol. 292). London: Home Office Research, Development and Statistics Directorate London.

Gill, M., & Turbin, V. (1998). CCTV and shop theft: towards a realistic evaluation. *Surveillance, closed circuit television and social control. Aldershot: Ashgate*, 189-206.

Givens, J. W., & Lam, D. (2019). Smarter Cities or Bigger Brother? How the Race for Smart Cities Could Determine the Future of China, Democracy, and Privacy. *Fordham Urb. LJ, 47*, 829.

Giyenko, A., & Im Cho, Y. (2016). *Intelligent UAV in smart cities using IoT.* Paper presented at the 2016 16th International Conference on Control, Automation and Systems (ICCAS).

Gjørv, G. H. (2012). Security by any other name: negative security, positive security, and a multi-actor security approach. *Review of international Studies, 38*(4), 835-859.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The discovery of grounded theory; strategies for qualitative research. *Nursing research, 17*(4), 364.

Glinsky, A. (2000). *Theremin: ether music and espionage.* Champaign, IL: University of Illinois Press.

Gohar, M., Muzammal, M., & Rahman, A. U. (2018). SMART TSS: Defining transportation system behavior using big data analytics in smart cities. *Sustainable cities and society, 41*, 114-119.

Goold, B. (2005). Unter dem Auge der Kamera: Closed Circuit Television und Polizeiarbeit. In L. Hempel & J. Metelmann (Eds.), *Bild-Raum-Kontrolle: Videoüberwachung als Zeichen des gesellschaftlichen Wandels* (pp. 221-234). Frankfurt am Main: Suhrkamp.

Goold, B. J. (2004). *CCTV and policing: Public area surveillance and police practices in Britain.* Oxford: Oxford University Press.

Gormley, K. (1992). One hundred years of privacy. *Wis. L. Rev.*, 1335.

Gough, D., Oliver, S., & Thomas, J. (2017). *An introduction to systematic reviews.* Thousand Oaks, CA: Sage.

Grace, J. (2019). 'Algorithmic Impropriety'in UK Policing Contexts: A Developing Narrative? *UK Policing Contexts: A Developing Narrative.* doi:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3487424

Graham, S. (1998). Towards the fifth utility? On the extension and normalisation of public CCTV. In C. Norris, J. Moran, & G. Armstrong (Eds.), *Surveillance, closed circuit television and social control* (pp. 89-112). Ashgate.

Graham, S. (2004). Postmortem city: towards an urban geopolitics. *City, 8*(2), 165-196.

Graham, S. (2005a). Switching cities off. *City, 9*(2), 169-194.

Graham, S. (2008). Robowar™ dreams: US military technophilia and global south urbanisation. *City, 12*(1), 25-49.

Graham, S. (2009). Cities as battlespace: The new military urbanism. *City, 13*(4), 383-402.

Graham, S. (2013). The new military urbanism *The Surveillance-Industrial Complex* (pp. 25-40): Routledge.

Graham, S., Brooks, J., & Heery, D. (1995). *Towns on the television: closed circuit TV surveillance in British towns and cities.* Newcastle upon Tyne: Department of Town and Country Planning, University of Newcastle upon Tyne.

Graham, S. D. (2005b). Software-sorted geographies. *Progress in human geography, 29*(5), 562-580.

Gras, M. (2001). Videoüberwachung in Großbritannien. *Neue Kriminalpolitik*, 12-15.

Gras, M. (2003). *Kriminalprävention durch Videoüberwachung: Gegenwart in Großbritannien - Zukunft in Deutschland?* Baden-Baden: Nomos.

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology, 53*(5), 864-885.

Greig-Midlane, J. (2019). An institutional perspective of neighbourhood policing reform in austerity era England and Wales. *International Journal of Police Science & Management, 21*(4), 230-243. doi:10.1177/1461355719889464

Greve, W., Leipold, B., & Kappes, C. (2018). Fear of Crime in Old Age: A Sample Case of Resilience? *The Journals of Gerontology: Series B, 73*(7), 1224-1232. doi:10.1093/geronb/gbw169

Groves, R. M., Singer, E., Lepkowski, J. M., Heeringa, S. G., & Alwin, D. F. (2004). Survey methodology. In J. S. House, F. T. Juster, R. L. Kahn, H. Schuman, & E. Singer (Eds.), *A telescope on society: Survey research and social science at the University of Michigan and beyond.* Ann Arbor: The University of Michigan Press.

Guan, L. (2012). Smart steps too a better city. *Government News, 32*(2), 24.

Gupta, A., Chakraborty, N., & Mondal, S. (2017). *CETD: An efficient clustering based energy theft detection technique in smart grid.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Habibzadeh, H., Soyata, T., Kantarci, B., Boukerche, A., & Kaptan, C. (2018). Sensing, communication and security planes: A new challenge for a smart city system design. *Computer Networks, 144*, 163-200.

Hackett, E. J., Amsterdamska, O., Lynch, M., & Wajcman, J. (2008). *The handbook of science and technology studies*: MIT Press Cambridge, MA.

Hadjkacem, B., Ayedi, W., Abid, M., & Snoussi, H. (2017). *A new method of video-surveillance data analytics for the security in camera networks.* Paper presented at the 2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC).

Haering, N., Venetianer, P. L., & Lipton, A. (2008). The evolution of video surveillance: an overview. *Machine Vision and Applications, 19*(5), 279-290.

Haggerty, K., & Ericson, R. (2005). *The new politics of surveillance and visibility.* Toronto: University of Toronto Press.

Haggerty, K. D. (2004). Displaced expertise: Three constraints on the policyrelevance of criminological thought. *Theoretical Criminology, 8*(2), 211-231.

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000). *The vision of a smart city.*

Hallinan, D., & Friedewald, M. (2012). Public Perception of Modern Surveillance Technologies: A Selected Survey Analysis of the Public Perception and Acceptance of New Surveillance Technologies. *Available at SSRN 2376651.*

Halperin, S., & Heath, O. (2017). *Political research: methods and practical skills.* Oxford: Oxford University Press.

Hara, M., Nagao, T., Hannoe, S., & Nakamura, J. (2016). New key performance indicators for a smart sustainable city. *Sustainability, 8*(3), 206.

Hardmeier, D., Hofer, F., & Schwaninger, A. (2005). *The X-ray object recognition test (X-ray ORT)-a reliable and valid instrument for measuring visual abilities needed in X-ray screening.* Paper presented at the Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on.

Harrell, K. (2014). *The Predictive Accuracy of Hotspot Mapping of Robbery over Time and Space.* University of Salford, Manchester.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for smarter cities. *IBM Journal of research and development, 54*(4), 1-16.

Hart, T. C., & Zandbergen, P. A. (2012). Effects of data quality on predictive hotspot mapping. *National Criminal Justice Reference Service.*

Hartama, D., Mawengkang, H., Zarlis, M., Sembiring, R. W., Furqan, M., Abdullah, D., & Rahim, R. (2017). *A research framework of disaster traffic management to Smart City.* Paper presented at the 2017 Second International Conference on Informatics and Computing (ICIC).

Hartzog, W., Conti, G., Nelson, J., & Shay, L. A. (2015). Inefficiently automated law enforcement. *Mich. St. L. Rev.*, 1763.

Hassell, K. D. (2006). *Police organizational cultures and patrol practices.* New York: LFB Scholarly Pub.

Hayes, T., & Mattimoe, R. (2004). To tape or not to tape: Reflections on methods of data collection. In C. Humphrey & B. Lee (Eds.), *The Real Life Guide to Accounting Research* (pp. 359-372). Amsterdam: Elsevier.

Heath, A., Evans, G., & Martin, J. (1994). The measurement of core beliefs and values: The development of balanced socialist/laissez faire and libertarian/authoritarian scales. *British Journal of Political Science, 24*(1), 115-132.

Hefendehl, R., & Stolle, P. (2002). Gefährliche Orte oder gefährliche Kameras? Die Videoüberwachung im öffentlichen Raum. *Kriminologisches Journal, 34*(4), 257-272.

Heger, N. (2010). Die Entwicklung der Sicherheitsgesellschaft am Beispiel der Videoüberwachung am Wiener Schwedenplatz *Wege der Sicherheitsgesellschaft* (pp. 343-357): Springer.

Hellen, N. (2021). £120 fines for litterbug drivers caught on camera. *The Times.* Retrieved from https://www.thetimes.co.uk/article/120-fines-for-litterbug-drivers-caught-on-camera-c522jkxxm

Helten, F., & Fischer, B. (2004). *What do people think about CCTV? Findings from a Berlin Survey*. Retrieved from

Hempel, L., & Bittner, P. (2007). Zur Evaluation von Videoüberwachung. In N. Zurawski (Ed.), *Surveillance Studies. Perspektiven eines Forschungsfeldes* (Vol. 1, pp. 117-147): Barbara Budrich.

Hempel, L., & Töpfer, E. (2002). Inception report. *Berlin: Technical University*.

Hempel, L., & Töpfer, E. (2004). CCTV in Europe. *Final report, 15*.

Hempel, L., & Töpfer, E. (2009). The surveillance consensus: Reviewing the politics of CCTV in three European countries. *European Journal of Criminology, 6*(2), 157-177.

Henchley, A., Knights, B., & Pascoe, T. (2002). Sustainability and Crime: Managing and Recognising the Drivers of Crime and Sustainability. *Watford: BRE*.

Henderson, C., & Izquierdo, E. (2016). Feature correspondence in low quality CCTV videos *Emerging Trends and Advanced Technologies for Computational Intelligence* (pp. 261-281): Springer.

Herrschel, T. (2013). Competitiveness and sustainability: can 'smart city regionalism'square the circle? *Urban Studies, 50*(11), 2332-2348.

Hier, S. P. (2011). *Panoptic dreams: Streetscape video surveillance in Canada*. Vancouver: UBC Press.

Higgins, G. E. (2016). Police Administration and Organisation. In W. G. Jennings & M. M. Maldonado-Molina (Eds.), *The Encyclopedia of Crime and Punishment* (Vol. 1). London: John Wiley & Sons.

Hillier, D., & Cozens, P. (2012). Revisiting Jane Jacobs's 'Eyes on the Street'for the Twenty-First Century: Evidence from Environmental Criminology *The Urban Wisdom of Jane Jacobs* (pp. 202-220): Routledge.

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review, 5*(3). doi:https://doi.org/10.14763/2016.3.424

Hirschmann, N., & Christe-Zeyse, J. (2016). Effective Change Management in the Police. *European Law Enforcement Research Bulletin*(1), 154-159. doi:https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/149

Hochstetler, J., Hochstetler, L., & Fu, S. (2016). *An optimal police patrol planning strategy for smart city safety*. Paper presented at the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

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

Hölscher, M. (2003). Sicherheitsgefühl und Überwachung. Eine empirische Studie zu Einstellungen der Bürger zur Videoüberwachung und ihrer erklärung. *Kriminologisches Journal, 35*(1), 42-56.

Hooghe, L., Bakker, R., Brigevich, A., De Vries, C., Edwards, E., Marks, G., . . . Vachudova, M. (2010). Reliability and validity of the 2002 and 2006 Chapel Hill expert surveys on party positioning. *European Journal of Political Research, 49*(5), 687-703.

Hosseini, M., Salehi, M. A., & Gottumukkala, R. (2017). *Enabling interactive video streaming for public safety monitoring through batch scheduling.* Paper presented at the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Hu, L., & Ni, Q. (2018). IoT-driven automated object detection algorithm for urban surveillance systems in smart cities. *IEEE Internet of Things Journal, 5*(2), 747-754.

Hu, W., Tan, T., Wang, L., & Maybank, S. (2004). A survey on visual surveillance of object motion and behaviors. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 34*(3), 334-352.

Huang, P.-R., & Chu, E. T.-H. (2017). *Indoor trapped-victim detection system.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Huberman, J. (2021). Amazon Go, surveillance capitalism, and the ideology of convenience. *Economic Anthropology.*

Huberman, M., & Miles, M. B. (2002). *The qualitative researcher's companion.* New York: Sage.

Huemer, M. (2013). The Logic of Predation. In M. Huemer (Ed.), *The Problem of Political Authority: An Examination of the Right to Coerce and the Duty to Obey* (pp. 198-229). London: Palgrave Macmillan UK.

Huston, S., Rahimzad, R., & Parsa, A. (2015). 'Smart'sustainable urban regeneration: Institutions, quality and financial innovation. *Cities, 48*, 66-75.

Ingram, J. R., Terrill, W., & Paoline III, E. A. (2018). Police culture and officer behavior: Application of a multilevel framework. *Criminology, 56*(4), 780-811.

Isafiade, O. E., & Bagula, A. B. (2017). *Fostering smart city development in developing nations: A crime series data analytics approach.* Paper presented at the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K).

Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspective. *International Journal of Information Management, 47*, 88-100.

ISO. (2018). ISO 31000 Risk management — Guidelines.

Italiano, R., Ramirez, F., & Chattopadhyay, S. (2021). Perceptions of police use of force among US adults and the role of communication accommodation in improving police–civilian interactions. *Journal of Applied Communication Research*, 1-18.

Iveson, K. (2010). The wars on graffiti and the new military urbanism. *City, 14*(1-2), 115-134.

Jackson, J., Bradford, B., Stanko, B., & Hohl, K. (2012). *Just authority?: Trust in the police in England and Wales.* London: Routledge.

Jalali, R., El-Khatib, K., & McGregor, C. (2015). *Smart city architecture for community level services through the internet of things.* Paper presented at the 2015 18th International Conference on Intelligence in Next Generation Networks.

Jayavadivel, R., & Prabaharan, P. (2021). Investigation on automated surveillance monitoring for human identification and recognition using face and iris biometric. *Journal of Ambient Intelligence and Humanized Computing*, 1-12.

Joh, E. E. (2007). Discretionless policing: technology and the Fourth Amendment. *Calif. L. Rev., 95*, 199.

Joh, E. E. (2013). Privacy protests: surveillance evasion and fourth amendment suspicion. *Ariz. L. Rev., 55*, 997.

Joh, E. E. (2017a). Automated policing. *Ohio St. J. Crim. L., 15*, 559.

Joh, E. E. (2017b). The Undue Influence of Surveillance Technology Companies in Policing. *NYUL Rev. Online, 92*, 19.

Joh, E. E. (2019a). Increasing automation in policing. *Communications of the ACM, 63*(1), 20-22.

Joh, E. E. (2019b). Policing the smart city. *International Journal of Law in Context, 15*(2), 177-182.

Joh, E. E. (2021). Policing, Race, & Technology. *University of Illinois Law Review, Forthcoming.*

Johnson, S. D., Summers, L., & Pease, K. (2006). Vehicle crime: Communicating spatial and temporal patterns.

Johnson, S. D., Tilley, N., & Bowers, K. J. (2015). Introducing EMMIE: an evidence rating scale to encourage mixed-method crime prevention synthesis reviews. *Journal of experimental criminology, 11*(3), 459-473.

Jöreskog, K. G. (1969). A general approach to confirmatory maximum likelihood factor analysis. *Psychometrika, 34*(2), 183-202.

Jun, S., Chang, T.-W., Jeong, H., & Lee, S. (2017). Camera Placement in Smart Cities for Maximizing Weighted Coverage with Budget Limit. *IEEE Sensors Journal, 17*(23), 7694-7703.

Kagawa, T., Saiki, S., & Nakamura, M. (2017). *Developing personalized security information service using open data.* Paper presented at the 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD).

Kagawa, T., Saiki, S., & Nakamura, M. (2018). Analyzing street crimes in Kobe city using PRISM. *International Journal of Web Information Systems.*

Kammerer, D. (2009). *Bilder der Überwachung* (2 ed.). Munich: Suhrkamp.

Kammerer, D. (2016). Überwachung *Handbuch Medien-und Informationsethik* (pp. 188-194): Springer.

Kane, R. J. (2002). The social ecology of police misconduct. *Criminology, 40*(4), 867-896.

Kankaanpää, A., Ariniemi, K., Heinonen, M., Kuoppasalmi, K., & Gunnar, T. (2016). Current trends in Finnish drug abuse: Wastewater based epidemiology combined with other national indicators. *Science of the Total Environment, 568*, 864-874.

Kappeler, V. E., & Kraska, P. B. (2015). Normalising police militarisation, living in denial. *Policing and Society, 25*(3), 268-275.

Karppi, T. (2018). “The computer said so”: On the ethics, effectiveness, and cultural techniques of predictive policing. *Social media+ society, 4*(2), 2056305118768296.

Kazig, R., Frank, J., & Reiter, T. (2006). Die alltägliche Wahrnehmung von Videoüberwachung: Konstruktionen und Handlungsrelevanz eines Kontrollinstruments öffentlicher Räume. In C. Wiegandt (Ed.), *Öffentliche Räume, öffentliche Träume. Zur Kontroverse über die Stadt und die Gesellschaft.* (pp. 61-72). Berlin: Springer.

Keenan, B. (2021). Automatic facial recognition and the intensification of police surveillance. *The Modern Law Review, 84*(4), 886-897.

Kerr, O. S. (2000). The fourth amendment in cyberspace: Can encryption create a reasonable expectation of privacy. *Conn. L. Rev., 33*, 503.

Keval, H., & Sasse, M. A. (2010). “Not the Usual Suspects”: a study of factors reducing the effectiveness of CCTV. *Security Journal, 23*(2), 134-154.

Khan, E. S., Azmi, H., Ansari, F., & Dhalvelkar, S. (2018). *Simple Implementation of Criminal Investigation using Call Data Records (CDRs) through Big Data Technology.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Khan, M. B. U., Aziz, M. B., Faruk, M. O., & Talukder, M. I. A. (2020). Impact of CCTV Surveillance on Crime Prevention: A Study in Dhaka City.

Khorov, E., Gushchin, A., & Safonov, A. (2015). *Distortion Avoidance While Streaming Public Safety Video in Smart Cities.* Paper presented at the International Workshop on Multiple Access Communications.

Kietzmann, J., & Angell, I. (2010). Panopticon revisited. *Communications of the ACM, 53*(6), 135-138.

Kim, H., Cha, Y., Kim, T., & Kim, P. (2020). *A study on the security threats and privacy policy of intelligent video surveillance system considering 5G network architecture.* Paper presented at the 2020 International Conference on Electronics, Information, and Communication (ICEIC).

Kim, S., & Lee, J. (2012). E-participation, transparency, and trust in local government. *Public Administration Review, 72*(6), 819-828.

Kirmeyer, S. L., & Dougherty, T. W. (1988). Work load, tension, and coping: Moderating effects of supervisor support. *Personnel Psychology, 41*(1), 125-139.

Kirschenbaum, A. A., Mariani, M., Van Gulijk, C., Rapaport, C., & Lubasz, S. (2012). Airports at risk: the impact of information sources on security decisions. *Journal of Transportation Security, 5*(3), 187-197.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1-14.

Kitchin, R., & Dodge, M. (2017). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 1-19. doi:10.1080/10630732.2017.1408002

Klauser, F. (2021). Surveillance and the smart city: Managing urban life through software.

Klauser, F. R. (2007). Difficulties in revitalizing public space by CCTV: Street prostitution surveillance in the Swiss city of Olten. *European Urban and Regional Studies, 14*(4), 337-348.

Klimczak, P., Kusche, I., Tschöpe, C., & Wolff, M. (2019). Menschliche und maschinelle Entscheidungsrationalität. Zur Kontrolle und Akzeptanz Künstlicher Intelligenz. *Zeitschrift für Medienwissenschaft, 11*(2), 39-45.

Klocke, G. (2001). Das Hintertürchen des nichtwissens. Was Regensburger BürgerInnen über die Videoüberwachung in ihrer stadt wissen und denken. *Bürgerrechte & Polizei/CILIP, 69*, 88-93.

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of social issues, 33*(3), 52-65.

Knockel, J., Crete-Nishihata, M., Ng, J. Q., Senft, A., & Crandall, J. R. (2015). *Every rose has its thorn: Censorship and surveillance on social video platforms in china.* Paper presented at the 5th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 15).

Kochel, T. R. (2018). Police legitimacy and resident cooperation in crime hotspots: effects of victimisation risk and collective efficacy. *Policing and Society, 28*(3), 251-270.

Komninos, N. (2006). The architecture of intelligent cities. *Intelligent Environments, 6*, 53-61.

Koskela, H. (2002). Video Surveillance, Gender, and the Safety of Public Urban Space: "Peeping Tom" Goes High Tech? *Urban Geography, 23*(3), 257-278. doi:10.2747/0272-3638.23.3.257

Koskela, H. (2003). 'Cam Era'—the contemporary urban Panopticon. *Surveillance & Society, 1*(3), 292-313.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kourtit, K., & Nijkamp, P. (2012). Smart cities in the innovation age. *Innovation: The European Journal of Social Science Research, 25*(2), 93-95.

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.

Krasmann, S. (2004). Die Kriminalität der Gesellschaft. Zur Gouvernementalität der Gegenwart. *Kriminologisches Journal, 36*(3), 229-230.

Krempel, E. L. (2016). *Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen*. Karlsruhe: KIT Scientific Publishing.

Krivý, M. (2018). Towards a critique of cybernetic urbanism: The smart city and the society of control. *Planning Theory, 17*(1), 8-30.

Kroll, J. A. (2018). The fallacy of inscrutability. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180084.

Krueger, B. S. (2005). Government Surveillance and Political Participation on the Internet. *Social science computer review, 23*(4), 439-452. doi:10.1177/0894439305278871

Kudlacek, D. (2015). *Akzeptanz von Videoüberwachung: eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen*. Berlin: Springer.

Kumar, S., Datta, D., Singh, S. K., & Sangaiah, A. K. (2018). An intelligent decision computing paradigm for crowd monitoring in the smart city. *Journal of Parallel and Distributed Computing, 118*, 344-358.

Kummitha, R. K. R., & Crutzen, N. (2017). How do we understand smart cities? An evolutionary perspective. *Cities, 67*, 43-52.

Kunst, R., Avila, L., Pignaton, E., Bampi, S., & Rochol, J. (2018). Improving network resources allocation in smart cities video surveillance. *Computer Networks, 134*, 228-244.

Kyba, C., Kuester, T., & Kuechly, H. (2017). Changes in outdoor lighting in Germany from 2012-2016. *International Journal of Sustainable Lighting, 19*(2), 112-123.

Kyprianides, A., Yesberg, J. A., Milani, J., Bradford, B., Quinton, P., & Clark–Darby, O. (2020). Perceptions of police use of force: the importance of trust. *Policing: An International Journal.*

La Vigne, N. G., Lowry, S. S., Dwyer, A. M., & Markman, J. A. (2011a). Using public surveillance systems for crime control and prevention: A practical guide for law enforcement and their municipal partners. *US Department of Justice. Recuperado el, 6.*

La Vigne, N. G., Lowry, S. S., Markman, J. A., & Dwyer, A. M. (2011b). Evaluating the use of public surveillance cameras for crime control and prevention. *Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.*

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *biometrics*, 159-174.

Lang, M. (2008). Private Videoueberwachung im oeffentlichen Raum. *Eine Untersuchung der Zulaessigkeit des privaten Einsatzes von Videotechnik und der Notwendigkeit von § 6b BDSG als spezielle rechtliche Regelung (German). Hamburg.*

Lauber, K., & Mühler, K. (2017). Ist das Vertrauen in die Institution Polizei eine Folge politischer Orientierungen? *Monatsschrift für Kriminologie und Strafrechtsreform/Journal of Criminology an Penal Reform, 100*(2), 87-102.

Lauer, J. (2012). Surveillance history and the history of new media: An evidential paradigm. *new media & society, 14*(4), 566-582.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social issues, 33*(3), 22-42.

Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, 14613557211064053. doi:10.1177/14613557211064053

Laufs, J., Borrion, H., & Bradford, B. (2020a). Security and the smart city: A systematic review. *Sustainable cities and society, 55*, 102023. doi:https://doi.org/10.1016/j.scs.2020.102023

Laufs, J., Bowers, K., Birks, D., & Johnson, S. (2020b). Understanding the Concept of 'Demand' in Policing: A Scoping Review and Resulting Implications for Demand Management. *Policing & Society, 31*(8), 895-918. doi:https://doi.org/10.1080/10439463.2020.1791862

Laufs, J., & Waseem, Z. (2020). Policing in Pandemics: A Systematic Review and Best Practices for Police Response to COVID-19. *International Journal of Disaster Risk Reduction*, 101812. doi:https://doi.org/10.1016/j.ijdrr.2020.101812

Lazaroiu, G. C., & Roscia, M. (2012). Definition methodology for the smart cities model. *Energy, 47*(1), 326-332.

Lee, H., Smeaton, A. F., O'Connor, N., & Murphy, N. (2005). *User-interface to a CCTV video search system*. Paper presented at the The IEE International Symposium on Imaging for Crime Detection and Prevention, London.

Lee, J., Kim, D., Ryoo, H.-Y., & Shin, B.-S. (2016). Sustainable wearables: Wearable technology for enhancing the quality of human life. *Sustainability, 8*(5), 466.

Lee, J., & Lee, H. (2014). Developing and validating a citizen-centric typology for smart city services. *Government Information Quarterly, 31*, S93-S105.

Lee, K., Quinn, P. C., & Pascalis, O. (2017). Face race processing and racial bias in early development: A perceptual-social linkage. *Current Directions in Psychological Science, 26*(3), 256-262.

Lee, N. T. (2018). Detecting racial bias in algorithms and machine learning. *Journal of Information, Communication and Ethics in Society*.

Leese, M. (2021). Security as Socio-Technical Practice: Predictive Policing and (Non-) Automation. *Swiss Political Science Review, 27*(1), 150-157.

Lei, J., Jiang, T., Wu, K., Du, H., Zhu, G., & Wang, Z. (2016). Robust K-means algorithm with automatically splitting and merging clusters and its applications for surveillance data. *Multimedia Tools and Applications, 75*(19), 12043-12059.

Leibold, J. (2020). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. *Journal of Contemporary China, 29*(121), 46-60.

Lella, J., Mandla, V. R., & Zhu, X. (2017). Solid waste collection/transport optimization and vegetation land cover estimation using Geographic Information System (GIS): A case study of a proposed smart-city. *Sustainable cities and society, 35*, 336-349.

Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European information society. *Journal of law and society, 31*(2), 194-220.

Leydesdorff, L., & Deakin, M. (2010). The triple helix model and the meta-stabilization of urban technologies in smart cities. *arXiv preprint arXiv:1003.3344*.

Li, C.-P. (2018). Exploring the gender difference in fear of crime among older people. *International Journal of Management, Economics and Social Sciences (IJMESS), 7*(Special Issue), 26-39.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Li, Y., Ren, L., & Luo, F. (2016). Is bad stronger than good? The impact of police-citizen encounters on public satisfaction with police. *Policing: An International Journal of Police Strategies & Management*.

Libbe, J. (2014). Smart City: Herausforderung für die Stadtentwicklung. Standpunkt.

Libbe, J. (2018). Intelligente Steuerung–Zur Umsetzung von Ansätzen smarter Städte und Regionen. In V. S., R. W., & W. G. (Eds.), *Handbuch zur Verwaltungsreform* (Vol. 1, pp. 571-580). Wiesbaden: Springer VS.

Liberatore, A. (2007). Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union. *European Journal on Criminal Policy and Research, 13*(1-2), 109-137.

Lim, S. S., Cho, H., & Sanchez, M. R. (2009). Online privacy, government surveillance and national ID cards. *Communications of the ACM, 52*(12), 116-120.

Lin, J., & Singer, P. (2016). China debuts Anbot, the police robot. *Popular science, 27*.

Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*. New Haven: Springer Science & Business Media.

Liotine, M., Ramaprasad, A., & Syn, T. (2016). *Managing a Smart City's Resilience to Ebola: An Ontological Framework*. Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Lischka, J. A. (2017). Explicit terror prevention versus vague civil liberty: How the UK broadcasting news (de) legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society, 20*(5), 665-682.

Liu, C.-B., & Ahuja, N. (2004). *Vision based fire detection*. Paper presented at the Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.

Liu, D., Lu, W., & Niu, Y. (2018). Extended technology-acceptance model to make smart construction systems successful. *Journal of Construction Engineering and Management, 144*(6), 04018035.

Liu, K., Warade, N., Pai, T., & Gupta, K. (2017a). *Location-aware smart campus security application*. Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Liu, Q., Lucas, K., & Marsden, G. (2020a). Public acceptability of congestion charging in Beijing, China: How transferrable are Western ideas of public acceptability? *International Journal of Sustainable Transportation, 15*(2), 97-110.

Liu, S., Ni, L. M., & Krishnan, R. (2014). Fraud detection from taxis' driving behaviors. *IEEE Transactions on Vehicular Technology, 63*(1), 464-472.

Liu, T., Mostafa, S., Mohamed, S., & Nguyen, T. S. (2020b). Emerging themes of public-private partnership application in developing smart city projects: a conceptual framework. *Built Environment Project and Asset Management, 11*(1), 138-156. doi:https://doi.org/10.1108/BEPAM-12-2019-0142

Liu, W.-C., & Lin, C.-H. (2017). *A hierarchical license plate recognition system using supervised K-means and Support Vector Machine*. Paper presented at the 2017 International Conference on Applied System Innovation (ICASI).

Liu, Y., Yu, L., Chi, T., Yang, B., Yao, X., Yang, L., . . . Cui, S. (2017b). *Design and implementation of community safety management oriented public information platform for a smart city*. Paper presented at the 2017 Forum on Cooperative Positioning and Service (CPGPS).

Lobsiger-Kägi, E., Weiss Sampietro, T., Eschenauer, U., Carabias-Hütter, V., Braunreiter, L., & Müller, A. W. (2016). Treiber und Barrieren auf dem Weg zu einer Smart City: Erkenntnisse aus Theorie und Praxis.

Lodge, J. (2007a). A Challenge for Privacy or Public Policy–Certified Identity and Uncertainties. *Regio-Minorities, Politics, Society-English Edition, 10*(1), 193-206.

Lodge, J. (2007b). Freedom, security and justice: the thin end of the wedge for biometrics? *ANNALI-ISTITUTO SUPERIORE DI SANITA, 43*(1), 20.

Lohokare, J., Dani, R., Sontakke, S., Apte, A., & Sahni, R. (2017). *Emergency services platform for smart cities.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Lombardi, P., Giordano, S., Caragliu, A., Del Bo, C., Deakin, M., Nijkamp, P., . . . Farouh, H. (2012a). An advanced triple-helix network model for smart cities performance *Regional Development: Concepts, Methodologies, Tools, and Applications* (pp. 1548-1562): IGI Global.

Lombardi, P., Giordano, S., Farouh, H., & Yousef, W. (2012b). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research, 25*(2), 137-149.

Lukpat, A. (2021). Amid cries of tyranny, England cancels plans to require vaccine passports. *New York Times.* Retrieved from https://www.nytimes.com/2021/09/12/world/europe/britain-vaccine-passport-cancelled.html

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly, 20*(2), 135-163.

Lung, C., Sabou, S., & Buchman, A. (2015). *Modelling and implementation of intelligent sensor networks with applications in emergency situations management.* Paper presented at the 2015 IEEE 21st International Symposium for Design and Technology in Electronic Packaging (SIITME).

Lyon, D. (2001). *Surveillance society: Monitoring everyday life.* London: McGraw-Hill Education (UK).

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination.* New York: Psychology Press.

Lyon, D. (2006). The search for surveillance theories *Theorizing surveillance* (pp. 17-34): Willan.

Ma, X., He, Y., Luo, X., Li, J., Zhao, M., An, B., & Guan, X. (2018). Camera Placement Based on Vehicle Traffic for Better City Security Surveillance. *IEEE Intelligent Systems, 33*(4), 49-61.

MacCallum, R. C., & Austin, J. T. (2000). Applications of structural equation modeling in psychological research. *Annual review of psychology, 51*(1), 201-226.

Macintosh, A. (2004). *Characterizing e-participation in policy-making.* Paper presented at the 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the.

Macnish, K. (2014). Just surveillance? Towards a normative theory of surveillance. *Surveillance & Society, 12*(1), 142-153.

Macnish, K., Wright, D., & Jiya, T. (2020). Predictive policing in 2025: A scenario *Policing in the Era of AI and Smart Societies* (pp. 199-215): Springer.

Madensen, T., Heskett, C., & Lieberman, J. (2012). *Predicting Crowd Behavior: A Response–Reaction Matrix.* Paper presented at the International Seminar on Environmental Criminology and Crime Analysis (ECCA) 21st International Symposium, Stavern, Norway.

Mahajan, M., Reddy, K., & Rajput, M. (2018). *A Switch Triggered Rescue Assistance System for Safety of Women.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Mamonov, S., & Koufaris, M. (2016). The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security, 12*(2), 56-67.

Manasa, N. (2016). *Nano Sensors and Pattern Recognition for Detection of Hidden Explosives.* Paper presented at the Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.

Mandl, B., & Schaner, P. (2012). *Der Weg zum Smart Citizen–soziotechnologische Anforderungen an die Stadt der Zukunft.* Paper presented at the REAL CORP 2012, 14-16 May 2012, Schwechat.

Mann, M., Mitchell, P., Foth, M., & Anastasiu, I. (2020). # BlockSidewalk to Barcelona: Technological sovereignty and the social license to operate smart cities. *Journal of the Association for Information Science and Technology, 71*(9), 1103-1115.

Manning, P. K. (2008). *The technology of policing: crime mapping, information technology, and the rationality of crime control* (Vol. 4). New York: NYU Press.

Manpearl, E. (2017). Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate. *U. Fla. JL & Pub. Pol'y, 28*, 65.

Marsal-Llacuna, M.-L. (2016). City indicators on social sustainability as standardization technologies for smarter (citizen-centered) governance of cities. *Social Indicators Research, 128*(3), 1193-1216.

Marshall, R. D., Bryant, R. A., Amsel, L., Suh, E. J., Cook, J. M., & Neria, Y. (2007). The psychology of ongoing threat: relative risk appraisal, the September 11 attacks, and terrorism-related fears. *American psychologist, 62*(4), 304.

Marx, G. T. (1995). The engineering of social control: The search for the silver bullet. *Crime and inequality*, 225-246.

Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society, 14*(3), 171-185.

Marx, G. T. (2015). Surveillance studies. *International encyclopedia of the social & behavioral sciences, 23*(2), 733-741.

Mastrobuoni, G. (2020). Crime is terribly revealing: Information technology and police productivity. *The Review of Economic Studies, 87*(6), 2727-2753.

Mata, F., Torres-Ruiz, M., Guzmán, G., Quintero, R., Zagal-Flores, R., Moreno-Ibarra, M., & Loza, E. (2016). A mobile information system based on crowd-sensed and official crime data for finding safe routes: A case study of mexico city. *Mobile Information Systems, 2016*.

Matos, A., Pinto, B., Barros, F., Martins, S., Martins, J., & Au-Yong-Oliveira, M. (2019). *Smart Cities and Smart Tourism: What Future Do They Bring?* Paper presented at the World Conference on Information Systems and Technologies.

Mazeika, D., & Summerton, D. (2017). The impact of geocoding method on the positional accuracy of residential burglaries reported to police. *Policing: An International Journal of Police Strategies & Management, 40*(2), 459-470.

McCahill, M. (1998). Beyond Foucault: towards a contemporary theory of surveillance. *Surveillance, closed circuit television and social control. Aldershot: Ashgate*, 41-65.

McCahill, M., & Norris, C. (2002). Urbaneye Working Paper No. 6-CCTV in London. *Urbaneye Webseite.*

McCahill, M., & Norris, C. (2003). Estimating the extent, sophistication and legality of CCTV in London. *CCTV*, 51-66.

McCoy, T., Bullock, R., & Brennan, P. (2005). RFID for airport security and efficiency.

McGuire, M. (2020). The laughing policebot: automation and the end of policing. *Policing and Society*, 1-17.

McLean, S. J., Worden, R. E., & Kim, M. (2013). Here's looking at you: An evaluation of public CCTV cameras and their effects on crime and disorder. *Criminal justice review, 38*(3), 303-334.

McLeod, S. (2007). Maslow's hierarchy of needs. *Simply psychology, 1.*

McQuade, S. (2006). Technology-enabled crime, policing and security. *The Journal of Technology Studies, 32*(1), 32-42.

Mehboob, F., Abbas, M., Rehman, S., Khan, S. A., Jiang, R., & Bouridane, A. (2017). Glyph-based video visualization on Google Map for surveillance in smart cities. *EURASIP Journal on Image and Video Processing, 2017*(1), 28.

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences, 82*(2), 392-408.

Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B.-G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems, 83*, 619-628.

Menichelli, F. (2014). Technology, context, users: a conceptual model of CCTV. *Policing: An International Journal of Police Strategies & Management.*

Metropolitan Police Service. (2017a). *The Met's Direction: Our Strategy 2018-2025.* Retrieved from https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/the-mets-direction---our-strategy-2018---2025.pdf

Metropolitan Police Service. (2017b). *ONE MET - Digital Policing Strategy.* Retrieved from https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/one-met-digital-policing-strategy-2017-2020.pdf

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology, 83*(2), 340-363.

Miles, M. B., & Huberman, A. M. (1984). Drawing valid meaning from qualitative data: Toward a shared craft. *Educational researcher, 13*(5), 20-30.

Milivojevic, S., & Radulski, E. M. (2020). The 'future Internet'and crime: towards a criminology of the Internet of Things. *Current Issues in Criminal Justice, 32*(2), 193-207.

Miraftabzadeh, S. A., Rad, P., Choo, K.-K. R., & Jamshidi, M. (2018). A Privacy-Aware Architecture at the Edge for Autonomous Real-Time Identity Reidentification in Crowds. *IEEE Internet of Things Journal, 5*(4), 2936-2946.

Mishra, D., & Kumar, M. (2013). Role of Technology in Smart Governance:'Smart City, Safe City'. *Safe City'(August 15, 2013).*

Mitchener-Nissen, T. (2013). Addressing social resistance in emerging security technologies. *Frontiers in human neuroscience, 7*, 483.

Mlinarić, A., Horvat, M., & Šupak Smolčić, V. (2017). Dealing with the positive publication bias: Why you should really publish your negative results. *Biochemia medica: Biochemia medica, 27*(3), 1-6.

Mohsin, K. (2020). Facial Recognition–Boon or Bane. *Available at SSRN 3666397.*

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.

Monahan, T. (2006). *Surveillance and security: Technological politics and power in everyday life*: Taylor & Francis.

Monahan, T., & Mokos, J. T. (2013). Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. *Geoforum, 49*, 279-288.

Moon, T.-H., Heo, S.-Y., Lee, S.-H., Leem, Y.-T., & Nam, K.-W. (2015). An analysis on the appropriateness and effectiveness of CCTV location for crime prevention. *World Acad. Sci. Eng. Tech. Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng, 9*(3), 836-843.

Moraes, T. G., Almeida, E. C., & de Pereira, J. R. L. (2021). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-) public spaces. *AI and Ethics, 1*(2), 159-172.

Morales, I., & Rubio Sánchez, R. (2017). Hacia una democracia plena de la mano de las tecnologías de la información y la comunicación.

Moreira, B., Cacho, N., Lopes, F., & Cavalcante, E. (2017). *Towards civic engagement in smart public security.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Morgan, A., & Dowling, C. (2019). Does CCTV help police solve crime? *Trends and Issues in Crime and Criminal Justice*(576), 1.

Morgan, H. M. (2013). Regulating CCTV?: We can't solve problems by using the same kind of thinking we used when we created them. *Critical Criminology, 21*(1), 15-30.

Moriuchi, E. (2021). An empirical study of consumers' intention to use biometric facial recognition as a payment method. *Psychology & Marketing.*

Morton, P. J., Horne, M., Dalton, R. C., & Thompson, E. M. (2012). Virtual city models: Avoidance of obsolescence. *Education and Research in Computer Aided Architectural Design in Europe-eCAADe, 1*, 213-224.

Mulligan, C. E., & Olsson, M. (2013). Architectural implications of smart city business models: an evolutionary perspective. *IEEE communications magazine, 51*(6), 80-85.

Murata, K., Adams, A. A., & Palma, A. M. L. (2017a). Following Snowden: a cross-cultural study on the social impact of Snowden's revelations. *Journal of Information, Communication and Ethics in Society, 15*(3), 183-196. doi:https://doi.org/10.1108/JICES-12-2016-0047

Murata, K., Fukuta, Y., Orito, Y., & Adams, A. A. (2017b). Few youngsters would follow Snowden's lead in Japan. *Journal of Information, Communication and Ethics in Society.*

Murgante, B., & Borruso, G. (2015). Cities and Smartness: The True Challenge Preface: IGI GLOBAL 701 E CHOCOLATE AVE, STE 200, HERSHEY, PA 17033-1240 USA.

Murphy, O. (2007). A surveillance society: Qualitative research report. *Wilmslow: ICO*.

Nagenborg, M. (2005). *Das Private unter den Rahmenbedingungen der IuK-Technologie*. Berlin: Springer.

Nam, J., Alghoniemy, M., & Tewfik, A. H. (1998). *Audio-visual content-based violent scene characterization*. Paper presented at the Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269).

Nam, T. (2017). Does ideology matter for surveillance concerns? *Telematics and Informatics, 34*(8), 1572-1585.

Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management, 38*(1), 262-269.

Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal, 56*(4), 530-544.

Nam, T., & Pardo, T. A. (2011). *Conceptualizing smart city with dimensions of technology, people, and institutions*. Paper presented at the Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times.

Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., & Morris, R. (2011). Smarter cities and their innovation challenges. *Computer, 44*(6), 32-39.

Nasui, D., Cernian, A., & Sgarciu, V. (2014). *Cloud based Student Transportation Safety System*. Paper presented at the Proceedings of the 2014 6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI).

National Police Chief's Council. (2016). *Policing Vision 2025*. Retrieved from https://www.npcc.police.uk/documents/Policing%20Vision.pdf

Nesterova, I. (2020). *Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world*. Paper presented at the SHS Web of Conferences.

Newell, B. C. (2013). Local law enforcement jumps on the big data bandwagon: Automated license plate recognition systems, information privacy, and access to government information. *Me. L. Rev., 66*, 397.

Newey, G. (2008). *Routledge philosophy guidebook to Hobbes and Leviathan*: Routledge.

Newman, O. (1972). *People and Design in the Violent City*. London: Architectural Press.

Neyland, D. (2006). *Privacy, surveillance and public trust*: Springer.

Neyroud, P., & Disley, E. (2008). Technology and policing: Implications for fairness and legitimacy. *Policing: A journal of policy and practice, 2*(2), 226-232.

Nguyen, D. H., Bedford, A., Bretana, A. G., & Hayes, G. R. (2011). *Situating the concern for information privacy through an empirical study of responses to video recording*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Nhan, J. (2014). Police culture. In A. J.S. (Ed.), *The encyclopedia of criminology and criminal justice* (pp. 1-6).

Nissen, T. G. (2014). *Designing for socially acceptable security technologies.* UCL (University College London).

Noor, N. M. M., Nawawi, W. M. F. W., & Ghazali, A. F. (2013). *Supporting decision making in situational crime prevention using fuzzy association rule.* Paper presented at the 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA).

Noor, P. (2020). Can we trust AI not to further embed racial bias and prejudice? *BMJ, 368*.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Norrie, A. (2002). Ethical and Social Perspectives in Situational Crime Prevention, Edited by A. Von Hirsch, D. Garland and A. Wakefield/The Judicial Role in Criminal Proceedings, Edited by S. Doran and J. Jackson. *King's Law Journal, 13*(1), 128-131.

Norris, C., & Armstrong, G. (1999). The Maximum Surveillance Society: The Rise of CCTV, Berg: Oxford.

Norris, C., & Armstrong, G. (2016). CCTV and the rise of mass surveillance society. In P. Carlen & R. Morgan (Eds.), *Crime Unlimited?: Questions for the Twenty-First Century*: Springer.

Norris, C., & Armstrong, G. (2020). *The maximum surveillance society: The rise of CCTV*: Routledge.

Norris, C., McCahill, M., & Wood, D. (2004). The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society, 2*(2/3).

Norris, C., & Moran, J. (2016). *Surveillance, closed circuit television and social control*: Routledge.

Oatley, G., Crick, T., & Bolt, D. (2015). *CCTV as a smart sensor network.* Paper presented at the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

Office for National Statistics. (2021). Principal projection - UK population in age groups. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationprojections/datasets/tablea21principalprojectionukpopulationinagegroups

Olive, E. W., Laube, R., & Hofer, F. (2009). *A comparison between two leadership models for security checkpoints.* Paper presented at the Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on.

Omrani, N., & Soulié, N. (2020). Privacy experience, privacy perception, political ideology and online privacy concern: the case of data collection in Europe. *Revue d'économie industrielle, 172*(4e).

Ostertagová, E., & Ostertag, O. (2013). Methodology and application of oneway ANOVA. *American Journal of Mechanical Engineering, 1*(7), 256-261.

Otway, H. J., & Von Winterfeldt, D. (1982). Beyond acceptable risk: On the social acceptability of technologies. *Policy sciences, 14*(3), 247-256.

Oxford Analytica. (2019). UK biometrics will accelerate amid mounting data risks. *Emerald Expert Briefings*(oxan-db).

Oza, N., & Gohil, N. (2016). *Implementation of cloud based live streaming for surveillance.* Paper presented at the 2016 International Conference on Communication and Signal Processing (ICCSP).

Painter, K. A., & Farrington, D. P. (2001). The financial benefits of improved street lighting, based on crime reduction. *Lighting Research & Technology, 33*(1), 3-10.

Papa, R., Galderisi, A., Vigo Majello, M. C., & Saretta, E. (2015). Smart and resilient cities. A systemic approach for developing cross-sectoral strategies in the face of climate change. *TeMA Journal of Land Use, Mobility and Environment, 8*(1), 19-49.

Parra, J., & Lopez, R. (2017). Application of predictive analytics for crime prevention: The case of the City of San Francisco *Police: Global Perceptions, Performance and Ethical Challenges* (pp. 85-109): Nova Science Publishers, Inc.

Parreno, J. B., & Demeterio III, F. P. A. (2012). Metacritique on Bentham and Foucault's Panoptic Theories as Analytic Tools for Three Modes of Digital Surveillance.

Pasquale, F. (2015). *The black box society*: Harvard University Press.

Patel, J., Wala, H., Shahu, D., & Lopes, H. (2018). *Intellectual and Enhance Digital Solution For Police Station.* Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Patterson, C. (2004). 'Technocorrections' and the future of crime control. *Criminal Justice Matters, 58*(1), 8-9.

Patton, J. W. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology, 2*(3), 181-187.

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science, 21*(5), 556-572.

Pavone, V., Santiago Gomez, E., & Jaquet-Chifelle, D.-O. (2016). A systemic approach to security: beyond the tradeoff between security and liberty. *Democracy and Security, 12*(4), 225-246.

Pechey, R., Burge, P., Mentzakis, E., Suhrcke, M., & Marteau, T. M. (2014). Public acceptability of population-level interventions to reduce alcohol consumption: a discrete choice experiment. *Social science & medicine, 113*, 104-109.

Peixoto, M. L., Souza, I., Barbosa, M., Lecomte, G., Batista, B. G., Kuehne, B. T., & Leite Filho, D. M. (2018). *Data Missing Problem in Smart Surveillance Environment.* Paper presented at the 2018 International Conference on High Performance Computing & Simulation (HPCS).

Pelton, J. N., & Singh, I. B. (2019). Coping with the dark web, cyber-criminals and techno-terrorists in a smart city *Smart cities of today and tomorrow* (pp. 171-183): Springer.

Peng, Z., Xiao, B., Yao, Y., Guan, J., & Yang, F. (2017). *U-safety: Urban safety analysis in a smart city.* Paper presented at the 2017 IEEE International Conference on Communications (ICC).

Pereira, R., Correia, D., Mendes, L., Rabadão, C., Barroso, J., & Pereira, A. (2018). *Low-Cost Smart Surveillance System for Smart Cities.* Paper presented at the International Conference on Universal Access in Human-Computer Interaction.

Perry, W. L. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*: Rand Corporation.

Petit, N. (2018). Artificial intelligence and automated law enforcement: A review paper. *Available at SSRN 3145133.*

Phillips, C., & Bowling, B. (2020). Racism, ethnicity, crime and criminal justice *Crime, Inequality and the State* (pp. 377-392): Routledge.

Piza, E. L. (2018). The crime prevention effect of CCTV in public places: a propensity score analysis. *Journal of Crime and Justice, 41*(1), 14-30.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014). Is the punishment more certain? An analysis of CCTV detections and enforcement. *Justice quarterly, 31*(6), 1015-1043.

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40‐year systematic review with meta‐analysis. *Criminology & Public Policy, 18*(1), 135-159.

Power, M. (2011). Foucault and sociology. *Annual Review of Sociology, 37*, 35-56.

Poyner, B. (1983). *Design against crime: Beyond defensible space*: Butterworths London.

Practical Androgyny. (2021). How many people in the United Kingdom are nonbinary? Retrieved from https://practicalandrogyny.com/2014/12/16/how-many-people-in-the-uk-are-nonbinary/

Pribadi, A., Kumiawan, F., Hariadi, M., & Nugroho, S. M. S. (2017). *Urban distribution CCTV for smart city using decision tree methods.* Paper presented at the 2017 International Seminar on Intelligent Technology and Its Applications (ISITIA).

Pryce, D. K., Wilson, G., & Fuller, K. (2018). Gender, age, crime victimization, and fear of crime: Findings from a sample of Kenyan College students. *Security Journal, 31*(4), 821-840.

Purtova, N. (2018). Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships. *International Data Privacy Law, 8*(1), 52-68. doi:https://doi.org/10.1093/idpl/ipx021

Qin, B., Strömberg, D., & Wu, Y. (2017). Why does China allow freer social media? Protests versus surveillance and propaganda. *Journal of Economic Perspectives, 31*(1), 117-140.

Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science, 48*(1), 137-141.

Ralko, S., & Kumar, S. (2016). Smart City Security.

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). *A unified definition of a smart city.* Paper presented at the International Conference on Electronic Government.

Rametta, C., Baldoni, G., Lombardo, A., Micalizzi, S., & Vassallo, A. (2017). S6: a Smart, Social and SDN-based Surveillance System for Smart-cities. *Procedia Computer Science, 110*, 361-368.

Ramírez, C. A., Barragán, R., García-Torales, G., & Larios, V. M. (2016). *Low-power device for wireless sensor network for Smart Cities*. Paper presented at the 2016 IEEE MTT-S Latin America Microwave Conference (LAMC).

Rankin, S., Cohen, N., Maclennan-Brown, K., & Sage, K. (2012). *CCTV operator performance benchmarking*. Paper presented at the 2012 IEEE International Carnahan Conference on Security Technology (ICCST).

Rao, B. N., Sudheer, R., Sadhanala, M. A., Tibirisettti, V., & Muggulla, S. (2020). *Movable Surveillance Camera using IoT and Raspberry Pi*. Paper presented at the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

Rasmussen, M. V. (2006). *The risk society at war: terror, technology and strategy in the twenty-first century*: Cambridge University Press.

Ratcliffe, J. (2006). *Video surveillance of public places*: Citeseer.

Ratcliffe, J. H. (2015). Towards an index for harm-focused policing. *Policing: A journal of policy and practice, 9*(2), 164-182.

Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. (2009). The crime reduction effects of public CCTV cameras: a multi-method spatial approach. *Justice quarterly, 26*(4), 746-770.

Rathore, M. M., Ahmad, A., Paul, A., & Rho, S. (2016). Urban planning and building smart cities based on the internet of things using big data analytics. *Computer Networks, 101*, 63-80.

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129-141.

Reddy, A. G., Suresh, D., Phaneendra, K., Shin, J. S., & Odelu, V. (2018a). Provably secure pseudo-identity based device authentication for smart cities environment. *Sustainable cities and society, 41*, 878-885.

Reddy, K. B. S., Loke, O., Jani, S., & Dabre, K. (2018b). *Tracking People In Real Time Video Footage Using Facial Recognition*. Paper presented at the 2018 International Conference on Smart City and Emerging Technology (ICSCET).

Reichardt, S. (2016). Einführung: Überwachungsgeschichte (n) Facetten eines Forschungsfeldes. *Geschichte und Gesellschaft, 42*(1), 5-33.

Reiner, R. (2010). *The politics of the police*: Oxford University Press.

Reisig, M. D., & Parks, R. B. (2000). Experience, quality of life, and neighborhood context: A hierarchical analysis of satisfaction with police. *Justice quarterly, 17*(3), 607-630.

Reuband, K.-H. (2001). Videoüberwachung: Was die Bürger von der Überwachung halten. *Neue Kriminalpolitik*, 5-9.

Reuter, C., Geilen, G., & Gellert, R. (2016). Sicherheit vs. Privatsphäre: Zur Akzeptanz von Überwachung in sozialen Medien im Kontext von Terrorkrisen. *Informatik 2016*.

Reynolds, J., Archer, S., Pilling, M., Kenny, M., Hollands, G. J., & Marteau, T. (2019). Public acceptability of nudging and taxing to reduce consumption of alcohol, tobacco, and food: A population-based survey experiment. *Social science & medicine, 236*, 112395.

Richards, N. M. (2012). The dangers of surveillance. *Harv. L. Rev., 126*, 1934.

Rigdon, E. E. (1996). CFI versus RMSEA: A comparison of two fit indexes for structural equation modeling. *Structural Equation Modeling: A Multidisciplinary Journal, 3*(4), 369-379.

Riley, T. (2007). Security vs. Privacy: A Comparative Analysis of Canada, the United Kingdom, and the United States. *Journal of Business and Public Policy, 1*(2), 1-21.

Ritchie, K. L., White, D., Kramer, R. S., Noyes, E., Jenkins, R., & Burton, A. M. (2018). Enhancing CCTV: Averages improve face identification from poor-quality images. *Applied Cognitive Psychology, 32*(6), 671-680.

Rocher, J., Taha, M., Parra, L., & Lloret, J. (2018). *IoT Sensor to Detect Fraudulent Use of Dyed Fuels in Smart Cities.* Paper presented at the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security.

Roesti, M. (2020). *"This is my Rifle"-On US Police Militarisation and Crime.* Retrieved from

Rogers, C., & Scally, E. J. (2018). Police use of technology: insights from the literature. *International Journal of Emergency Services, 7*(2), 100-110.

Rohstein, H., & Hopewell, S. (2009). Grey Literature. In H. Cooper, L. V. Hedges, & J. Valentine (Eds.), *Handbook of Research on Adult Learning and Development* (2nd ed., pp. 184-202): Routledge.

Roman, J., & Farrell, G. (2002). Cost-benefit analysis for crime prevention: opportunity costs, routine savings and crime externalities.

Rossler, M. T. (2019). The impact of police technology adoption on social control, police accountability, and police legitimacy *Political Authority, Social Control and Public Policy*: Emerald Publishing Limited.

Roßnagel, A., Desoi, M., & Hornung, G. (2011). Gestufte Kontrolle bei Videoüberwachungsanlagen. *Datenschutz und Datensicherheit-DuD, 35*(10), 694.

Rothe, M. (2003). Big Brother im Panopticon? Überwachung aus liberaler und aus autonomiekritischer Sicht. *Grötker, Ralf (Hg.): Privat*, 33-42.

Rothkrantz, L. (2017a). *Lip-reading by surveillance cameras.* Paper presented at the 2017 Smart City Symposium Prague (SCSP).

Rothkrantz, L. (2017b). *Person identification by smart cameras.* Paper presented at the 2017 Smart City Symposium Prague (SCSP).

Rothmann, R. (2010). Sicherheitsgefühl durch Videoüberwachung? Argumentative Paradoxien und empirische Widersprüche in der Verbreitung einer sicherheitspolitischen Maßnahme. *Neue Kriminalpolitik, 22*(3), 103-107.

Rötzer, F. (2015). *Smart cities im Cyberwar*: Westend Verlag.

Rowntree, D. (2000). *Statistics Without Tears: An Introduction for Non-mathematicians*: Penguin.

Rutakumwa, R., Mugisha, J. O., Bernays, S., Kabunga, E., Tumwekwase, G., Mbonye, M., & Seeley, J. (2020). Conducting in-depth interviews with and without voice recorders: a comparative analysis. *Qualitative Research, 20*(5), 565-581.

Saba, A. (2017). *IOT based energy efficient security system.* Paper presented at the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

Sabbagh, D. (2019). Facial recognition row: police gave King's Cross owner images of seven people. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people

Sacchi, C., & Regazzoni, C. S. (2000). A distributed surveillance system for detection of abandoned objects in unmanned railway environments. *IEEE Transactions on Vehicular Technology, 49*(5), 2013-2026.

Sadgali, I., Sael, N., & Benabbou, F. (2018). Detection of credit card fraud: State of art. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18*(11), 76-83.

Saetnan, A. R., Dahl, J. Y., & Lomell, H. M. (2004). Views from under surveillance. Public opinion in a closely watched area in Oslo. *Urbaneye Project.*

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., . . . Baik, S. W. (2017). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Generation Computer Systems.*

Sajjad, M., Nasir, M., Ullah, F. U. M., Muhammad, K., Sangaiah, A. K., & Baik, S. W. (2018). Raspberry Pi assisted facial expression recognition framework for smart security in law-enforcement services. *Information Sciences, 479*, 416-431.

Salder, F. (2020). Kommunale Videosicherheitstechnik im Aufbruch: von der Verbrechensbekämpfung zum „Smart-City-Sensor " *Smart City–Made in Germany* (pp. 717-726): Springer.

Salmerón-García, J. J., van den Dries, S., Díaz-del-Río, F., Morgado-Estevez, A., Sevillano-Ramos, J. L., & van de Molengraft, M. (2017). Towards a cloud-based automated surveillance system using wireless technologies. *Multimedia Systems*, 1-15.

Salter, M. (2014). Toys for the boys? Drones, pleasure and popular culture in the militarisation of policing. *Critical Criminology, 22*(2), 163-177.

Sandborn, P. (2007). *Designing for technology obsolescence management.* Paper presented at the IIE Annual Conference. Proceedings.

Sanders, C., & Henderson, S. (2013). Integrated policing and information sharing: Functional, ideological and organizational barriers to police technologies. *Policing and Society: An International Journal, 23*, 243-260.

Sanders, C. B., & Hannem, S. (2012). Policing "the risky": Technology and surveillance in everyday patrol work. *Canadian Review of Sociology/Revue canadienne de sociologie, 49*(4), 389-410.

Sanders, C. B., Weston, C., & Schott, N. (2015). Police innovations,'secret squirrels' and accountability: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology, 55*(4), 711-729.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society, 31*(1), 66-81.

Sarasin, P. (2016). *Michel Foucault zur Einführung* (Vol. 333): Junius.

Saravanakumar, K., Deepa, K., & Kumar, N. S. (2017). *A study on possible application of RFID system in different real-time environments.* Paper presented at the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT).

Saris, W. E., Satorra, A., & Van der Veld, W. M. (2009). Testing structural equation models or detection of misspecifications? *Structural Equation Modeling, 16*(4), 561-582.

Sarkissian, W., & Wenman, C. (2010). *Creative community planning: Transformative engagement methods for working at the edge*: Routledge.

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. (2018). Responding to cybercrime: current trends: Taylor & Francis.

Schafer, J. A., Huebner, B. M., & Bynum, T. S. (2003). Citizen perceptions of police services: Race, neighborhood context, and community policing. *Police Quarterly, 6*(4), 440-468.

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review, 27*(1), 45-52.

Scheuer, D. (2020a). Beobachtungsstudie zur Akzeptanz Künstlicher Intelligenz *Akzeptanz von Künstlicher Intelligenz* (pp. 67-137): Springer.

Scheuer, D. (2020b). Entwicklung eines Theoriemodells zur Akzeptanz von Künstlicher Intelligenz *Akzeptanz von Künstlicher Intelligenz* (pp. 57-65): Springer.

Schmidt, T., Philipsen, R., & Ziefle, M. (2015). *From v2x to control2trust.* Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust.

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), 13.

Schuilenburg, M. B., & Steden, R. v. (2014). *Positive security: a theoretical framework*: Eleven.

Schuitema, G., Steg, L., & Forward, S. (2010). Explaining differences in acceptability before and acceptance after the implementation of a congestion charge in Stockholm. *Transportation Research Part A: Policy and Practice, 44*(2), 99-109.

Schuman, H., & Presser, S. (1996). *Questions and answers in attitude surveys: Experiments on question form, wording, and context*: Sage.

Seddon, T. (2004). Searching for the next techno-fix: Drug testing in the criminal justice system. *Criminal Justice Matters, 58*(1), 16-17.

Sedky, M. H., Moniri, M., & Chibelushi, C. C. (2005). *Classification of smart video surveillance systems for commercial applications.* Paper presented at the IEEE Conference on Advanced Video and Signal Based Surveillance, 2005.

Selmini, R. (2004). *La sicurezza urbana*: Il Mulino.

Sen, M., Dutt, A., Agarwal, S., & Nath, A. (2013). *Issues of privacy and security in the role of software in smart cities.* Paper presented at the Communication Systems and Network Technologies (CSNT), 2013 International Conference on.

Shapiro, J. M. (2006). Smart cities: quality of life, productivity, and the growth effects of human capital. *The review of economics and statistics, 88*(2), 324-335.

Shearing, C., & Stenning, P. (1985). From the panopticon to Disney World: The development of discipline. *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards. Toronto: Canada Law Book*, 335-349.

Sheldon, B. (2011). Camera surveillance within the UK: Enhancing public safety or a social threat? *International review of law, computers & technology, 25*(3), 193-203.

Shelton, T., Zook, M., & Wiig, A. (2015). The 'actually existing smart city'. *Cambridge Journal of Regions, Economy and Society, 8*(1), 13-25.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L., & Hong, J. (2009). *Improving phishing countermeasures: An analysis of expert interviews.* Paper presented at the 2009 eCrime Researchers Summit.

Sherman, L. W. (2007). The power few: experimental criminology and the reduction of harm. *Journal of experimental criminology, 3*(4), 299-321.

Shi, J., Ming, Y., Fan, C., & Tian, L. (2017). *Face recognition algorithm based on multi-scale CLBP.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Silverman, E. B., & Della-Giustina, J.-A. (2001). Urban policing and the fear of crime. *Urban Studies, 38*(5-6), 941-957.

Sindall, K., & Sturgis, P. (2013). Austerity policing: Is visibility more important than absolute numbers in determining public confidence in the police? *European Journal of Criminology, 10*(2), 137-153.

Singh, A., Patil, D., & Omkar, S. (2018). Eye in the Sky: Real-time Drone Surveillance System (DSS) for Violent Individuals Identification using ScatterNet Hybrid Deep Learning Network. *arXiv preprint arXiv:1806.00746.*

Singh, G., Majumdar, S., & Rajan, S. (2017). *MapReduce-based techniques for multiple object tracking in video analytics.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Siregar, A. H., Syahputra, D., Putra, D. A., & Wicaksono, B. (2018). *Policy Evaluation of Security System Based on Security Camera Technology in Batam City.* Paper presented at the IOP Conference Series: Earth and Environmental Science.

Skogan, W. G. (2005). Citizen satisfaction with police encounters. *Police Quarterly, 8*(3), 298-321.

Skogan, W. G. (2019). The future of CCTV. *Criminology & Public Policy, 18*(1), 161-166.

Skoy, E. (2021). Black Lives Matter Protests, Fatal Police Interactions, and Crime. *Contemporary Economic Policy, 39*(2), 280-291.

Slee, R. (2004). CHAPTER 3: MEANING IN THE SERVICE OF POWER. *Counterpoints, 270*, 46-60.

Smith, A. D. (2005). Gauging acceptability of governmental intervention in terms of smart card technology. *Electronic Government, an International Journal, 2*(1), 87-110.

Smith, G. J. (2020). The politics of algorithmic governance in the black box city. *Big Data & Society, 7*(2), 2053951720933989.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Smith, M. J., & Clarke, R. V. (2000). Crime and public transport. *Crime and Justice, 27*, 169-233.

Smyth, S. M. (2019). The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech? *International Journal of Cyber Criminology, 13*(2), 578-595.

Söderström, O., Paasche, T., & Klauser, F. (2014). Smart cities as corporate storytelling. *City, 18*(3), 307-320.

Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I., & Tisato, F. (2016). A serious game empowering the prediction of potential terrorist actions. *Journal of Policing, Intelligence and Counter Terrorism, 11*(1), 30-48.

Sousa, W. H., & Madensen, T. D. (2016). Citizen acceptance of police interventions: an example of CCTV surveillance in Las Vegas, Nevada. *Criminal Justice Studies, 29*(1), 40-56.

Spence, K. (2005). World risk society and war against terror. *Political Studies, 53*(2), 284-302.

Spriggs, A., Argomaniz, J., Gill, M., & Bryan, J. (2005). Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV. *Home Office Online Report, 10*(05).

Srivastava, M., Abdelzaher, T., & Szymanski, B. (2012). Human-centric sensing. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 370*(1958), 176-197.

Steinbock, D. J. (2005). Data matching, data mining, and due process. *Ga. L. Rev., 40*, 1.

Stelfox, P. (2013). *Criminal investigation: An introduction to principles and practice*: Routledge.

Stierand, P. (2000). *Videoüberwachte Stadt?: sichere öffentliche Räume als Aufgabe der Stadtplannung*: Fakultät Raumplanung.

Straube, T., & Belina, B. (2018). Policing the Smart City: Eine Taxonomie polizeilicher Prognoseprogramme *Smart City-Kritische Perspektiven auf die Digitalisierung in Städten* (pp. 223-236): transcript-Verlag.

Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American society for information science and technology, 56*(3), 221-234.

Struyf, P. (2020). Fear of the dark: The potential impact of reduced street lighting on crime and fear of crime 1. *Crime and fear in public places*, 347-361.

Sudha, N. (2015). *Enabling Seamless Video Processing in Smart Surveillance Cameras with Multicore.* Paper presented at the 2015 International Conference on Advanced Computing and Communications (ADCOM).

Sugaris, A. (2020). 5G Edge-Based Video Surveillance in Smart Cities *5G Multimedia Communication* (pp. 299-320): CRC Press.

Summers, L., & Johnson, S. D. (2017). Does the configuration of the street network influence where outdoor serious violence takes place? Using space syntax to test crime pattern theory. *Journal of quantitative criminology, 33*(2), 397-420.

Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & society review, 37*(3), 513-548.

Surveillance Camera Commissioner. (2016). *Annual Report 2015/16.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/569559/57586_unnum_camera_WEB.PDF.

Surveillance Camera Commissioner. (2017). *A National Surveillance Strategy for England and Wales.* Retrieved from https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales.

Surveillance Camera Commissioner. (2020). *National Surveillance Camera Strategy Objectives 2020 – 2023.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881604/National_Surveillance_Camera_Objectives_2020_-_2023.pdf.

Sutriadi, R. (2018). *Defining smart city, smart region, smart village, and technopolis as an innovative concept in Indonesia's urban and regional development themes to reach sustainability.* Paper presented at the IOP Conference Series: Earth and Environmental Science.

Sweet, K. (2008). *Aviation and airport security: terrorism and safety concerns*: CRC Press.

Tan, H., & Chen, L. (2014). *An approach for fast and parallel video processing on Apache Hadoop clusters.* Paper presented at the 2014 IEEE International Conference on Multimedia and Expo (ICME).

Tao, J., Turjo, M., Wong, M.-F., Wang, M., & Tan, Y.-P. (2005). *Fall incidents detection for intelligent video surveillance.* Paper presented at the 2005 5th International Conference on Information Communications & Signal Processing.

Taylor, B., Kowalyk, A., & Boba, R. (2007). The integration of crime analysis into law enforcement agencies: An exploratory study into the perceptions of crime analysts. *Police Quarterly, 10*(2), 154-169.

Taylor, E., & Lee, M. (2019). Off the record?: Arrestee concerns about the manipulation, modification, and misrepresentation of police body-worn camera footage. *Surveillance and society, 17*(3-4), 474-483.

Taylor, R. B., Gottfredson, S. D., & Brower, S. (1984). Block crime and fear: Defensible space, local social ties, and territorial functioning. *Journal of Research in crime and delinquency, 21*(4), 303-331.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*: Prentice Hall Press.

Thierer, A. (2013). The pursuit of privacy in a world where information control is failing. *Harv. JL & Pub. Pol'y, 36*, 409.

Thite, M. (2011). Smart cities: implications of urban planning for human resource development. *Human Resource Development International, 14*(5), 623-631.

Thomas, A. L., Piza, E. L., Welsh, B. C., & Farrington, D. P. (2021). The internationalisation of cctv surveillance: Effects on crime and implications for emerging technologies. *International Journal of Comparative and Applied Criminal Justice*, 1-22.

Thomas, J., O'Mara-Eves, A., Harden, A., & Newman, M. (2017a). Synthesis Methods for Combining and Configuring Quantitative Data. In D. Gough, S. Oliver, & J. Thomas (Eds.), *An Introduction to Systematic Reviews* (2nd ed., pp. 181-211). London: SAGE Publications.

Thomas, S. S., Gupta, S., & Subramanian, V. K. (2017b). *Smart surveillance based on video summarization.* Paper presented at the 2017 IEEE Region 10 Symposium (TENSYMP).

Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology, 71*(9), 1129-1142.

Thuzar, M. (2011). Urbanization in Southeast Asia: developing smart cities for the future? *Regional Outlook*, 96.

Thys, S., Van Ranst, W., & Goedemé, T. (2019). *Fooling automated surveillance cameras: adversarial patches to attack person detection.* Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

Tian, L., Wang, H., Zhou, Y., & Peng, C. (2018). Video big data in smart city: Background construction and optimization for surveillance video processing. *Future Generation Computer Systems, 86*, 1371-1382.

Tien, L. (2004). Privacy, technology and data mining. *Ohio NUL Rev., 30*, 389.

Tilley, N. (1993). *Understanding Car Parks, Crime and CCTV: Evaluation Lessons From Safer Cities.* Retrieved from Home Office Police Research Group: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.518.3703&rep=rep1&type=pdf

Töpfer, E. (2004). Videoüberwachung im europäischen Vergleich. Gemeinsame Trend und nationale Unterschiede (Vortrag für den 21. Chaos Communication Congress in Berlin, 27. Dezember 2004): Internetquelle.

Töpfer, E. (2005). Die polizeiliche Videoüberwachung des öffentlichen Raums: Entwicklung und Perspektiven. *Beitrag für „DANA Datenschutznachrichten "(Themenheft: Staatliche Überwachung).*

Toppeta, D. (2010). The smart city vision: how innovation and ICT can build smart,"livable", sustainable cities. *The Innovation Knowledge Foundation. Think.*

Tourangeau, R., & Smith, T. W. (1996). Asking sensitive questions: The impact of data collection mode, question format, and question context. *Public opinion quarterly, 60*(2), 275-304.

Townsend, A. M. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*: WW Norton & Company.

Treibel, A., Korte, H., & Schäfers, B. (1997). Einführung in soziologische Theorien der Gegenwart.

Trinkner, R., Jackson, J., & Tyler, T. R. (2018). Bounded authority: Expanding "appropriate" police behavior beyond procedural justice. *Law and Human Behavior, 42*(3), 280.

Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421-433.

Truntsevsky, Y. V., Lukiny, I., Sumachev, A., & Kopytova, A. (2018). *A smart city is a safe city: the current status of street crime and its victim prevention using a digital application.* Paper presented at the MATEC Web of Conferences.

Tsoukala, A. (2006). Democracy in the light of security: British and French political discourses on domestic counter-terrorism policies. *Political Studies, 54*(3), 607-627.

Tucker, L. R., & Lewis, C. (1973). A reliability coefficient for maximum likelihood factor analysis. *Psychometrika, 38*(1), 1-10.

Tung, G. (2021). Technology as a Tool for Transnational Organized Crime: Networking and Money Laundering. *The Journal of Intelligence, Conflict, and Warfare, 4*(1), 112-121.

Turtiainen, H., Costin, A., Hamalainen, T., & Lahtinen, T. (2020). Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision. Applications and implications for privacy, safety, and cybersecurity.(Preprint). *arXiv preprint arXiv:2006.03870.*

Tyler, T. R. (2021). *Why People Obey the Law*: Princeton University Press.

Udoh, E. S. (2020). *Is the data fair? An assessment of the data quality of algorithmic policing systems.* Paper presented at the Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance.

United Nations. (2018). *World Urbanization Prospects 2018.* New York: United Nations, Retrieved from https://population.un.org/wup/.

Valentín, L., Serrano, S. A., García, R. O., Andrade, A., Palacios-Alonso, M. A., & Sucar, L. E. (2017). A CLOUD-BASED ARCHITECTURE FOR SMART VIDEO SURVEILLANCE. *International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences, 42.*

Valentino, N. A., Neuner, F. G., Kamin, J., & Bailey, M. (2021). Testing Snowden's HypothesisDoes Mere Awareness Drive Opposition to Government Surveillance? *Public opinion quarterly.*

Van Damme, A. (2017). The impact of police contact on trust and police legitimacy in Belgium. *Policing and Society, 27*(2), 205-228.

van Heek, J., Aming, K., & Ziefle, M. (2016). *"How fear of crime affects needs for privacy & safety": Acceptance of surveillance technologies in smart cities.* Paper presented at the Smart Cities and Green ICT Systems (SMARTGREENS), 2016 5th International Conference on.

van Heek, J., Arning, K., & Ziefle, M. (2017) The surveillance society: Which factors form public acceptance of surveillance technologies? *: Vol. 738* (pp. 170-191): Springer Verlag.

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

Vanolo, A. (2014). Smartmentality: The smart city as disciplinary strategy. *Urban Studies, 51*(5), 883-898.

Vanolo, A. (2016). Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures, 82*, 26-36.

Venkatesan, S., Jawahar, A., Varsha, S., & Roshne, N. (2017). *Design and implementation of an automated security system using Twilio messaging service.* Paper presented at the 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS).

Viera, A. J., & Garrett, J. M. (2005). Understanding interobserver agreement: the kappa statistic. *Fam med, 37*(5), 360-363.

Vinod Kumar, T. (2014). Differing services, rising expectations, and greater demands: patterns in variations of police-public dynamics across areas with conventional and community policing in India. *Policing: An International Journal of Police Strategies & Management, 37*(1), 170-189.

Vitalij, F., Robnik, A., & Alexey, T. (2012). " Safe City"-an Open and Reliable Solution for a Safe and Smart City. *Elektrotehniski Vestnik, 79*(5), 262.

Von Hirsch, A., Garland, D., & Wakefield, A. (2000). *Ethical and social perspectives on situational crime prevention* (Vol. 1): Hart Publishing.

von Lucke, J. (2020). Wie smart darf Polizeiarbeit eigentlich werden? *VM Verwaltung & Management, 26*(3), 107-124.

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* (Vol. 1): Hart Publishing.

Wang, J., Pan, J., & Esposito, F. (2017). *Elastic urban video surveillance system using edge computing.* Paper presented at the Proceedings of the Workshop on Smart Internet of Things.

Wang, X. (2013). Intelligent multi-camera video surveillance: A review. *Pattern recognition letters, 34*(1), 3-19.

Wankhede, K., Wukkadada, B., & Nadar, V. (2018). *Just walk-out technology and its challenges: A case of Amazon Go.* Paper presented at the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA).

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

Watzinger, G. (2019). *Smart City: Sicherheits-und Überwachungstechnologien und deren Einfluss auf das subjektive Sicherheitsgefühl im öffentlichen Raum.* Wien.

WCED. (1987). *Our common future* (Vol. 17). Oxford: Oxford University Press.

Webb, M. (2007). *Illusions of security: Global surveillance and democracy in the post-9/11 world*: City Lights Books.

Webster, C. W. R. (2009). CCTV policy in the UK: reconsidering the evidence base. *Surveillance and society, 6*(1), 10-22.

Wehrheim, J. (2012). *Die überwachte Stadt – Sicherheit, Segregation und Ausgrenzung*: Verlag Barbara Budrich.

Weisburd, D., & Braga, A. A. (2019). *Police innovation: Contrasting perspectives*: Cambridge University Press.

Weisburd, D., Majmundar, M. K., Aden, H., Braga, A., Bueermann, J., Cook, P. J., . . . Lum, C. (2019). Proactive policing: A summary of the report of the National Academies of Sciences, Engineering, and Medicine. *Asian Journal of Criminology, 14*(2), 145-177.

Weiss, B., Caron, A., Ball, S., Tapp, J., Johnson, M., & Weisz, J. R. (2005). Iatrogenic effects of group treatment for antisocial youths. *Journal of consulting and clinical psychology, 73*(6), 1036.

Weitzer, R., & Tuch, S. A. (2005). Racially biased policing: Determinants of citizen perceptions. *Social forces, 83*(3), 1009-1030.

Wells, H. (2008). The techno-fix versus the fair cop: Procedural (in) justice and automated speed limit enforcement. *The British Journal of Criminology, 48*(6), 798-817.

Wells, W. (2007). Type of contact and evaluations of police officers: The effects of procedural justice across three types of police–citizen contacts. *Journal of Criminal Justice, 35*(6), 612-621.

Welsh, B. C., & Farrington, D. P. (2002). *Crime prevention effects of closed circuit television: a systematic review* (Vol. 252): Citeseer.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice quarterly, 26*(4), 716-745.

Welsh, B. C., & Rocque, M. (2014). When crime prevention harms: A review of systematic reviews. *Journal of experimental criminology, 10*(3), 245-266.

Welsh, D., & Roy, N. (2017). *Smartphone-based mobile gunshot detection.* Paper presented at the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).

Welsh, J. S., & Kong, H. (2011). Robust experiment design through randomisation with chance constraints. *IFAC Proceedings Volumes, 44*(1), 13197-13202.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008). Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. *HAISA, 8*, 35-48.

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies, 67*(7), 584-606.

West, S. G., Taylor, A. B., & Wu, W. (2012). Model fit and model selection in structural equation modeling. *Handbook of structural equation modeling, 1*, 209-231.

Westin, A. F. (1967). Privacy and Freedom (London: The Bodley Head). *WestinPrivacy and Freedom1967.*

Wexler, R. (2018). Life, liberty, and trade secrets: Intellectual property in the criminal justice system. *Stan. L. Rev., 70*, 1343.

Wheeler, C. A. (2016). Barriers to community development in distressed cities: A case study of Camden, New Jersey. *Community Development, 47*(4), 496-513.

White, L., Harris, S., Joseph-Salisbury, R., & Williams, P. (2021). A Collision of Crises: Racism, Policing, and the COVID-19 Pandemic.

White, M. D., & Escobar, G. (2008). Making good cops in the twenty-first century: Emerging issues for the effective recruitment, selection and training of police in the United States and abroad. *International review of law, computers & technology, 22*(1-2), 119-134.

Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale LJ, 113*, 1151.

Wiig, A. (2018). Secure the city, revitalize the zone: Smart urbanization in Camden, New Jersey. *Environment and Planning C: Politics and Space, 36*(3), 403-422.

Wiliem, A., Madasu, V., Boles, W., & Yarlagadda, P. (2012). A suspicious behaviour detection using a context space model for smart surveillance systems. *Computer Vision and Image Understanding, 116*(2), 194-209.

Willems, J., Van den Bergh, J., & Viaene, S. (2017). Smart city projects and citizen participation: The case of London *Public Sector Management in a Globalized World* (pp. 249-266): Springer.

Williams, K. S., & Johnstone, C. (2000). The politics of the selective gaze: closed circuit television and the policing of public space. *Crime, Law and Social Change, 34*(2), 183-210.

Willis, J. J. (2014). A recent history of the police. *The Oxford handbook of police and policing*, 3-33.

Willis, M., Taylor, E., & Lee, M. (2017). Police detainee perspectives on CCTV. *Trends and Issues in Crime and Criminal Justice [electronic resource]*(538), 1-14.

Wilson, D. (2019). Predictive Policing Management: A Brief History of Patrol Automation. *New Formations, 98*(98), 139-155.

Wilson, D. B. (2009). Missing a critical piece of the pie: simple document search strategies inadequate for systematic reviews. *Journal of experimental criminology, 5*(4), 429-440.

Wilson, J. M., & Weiss, A. (2014). Police staffing allocation and managing workload demand: a critical assessment of existing practices. *Policing: A journal of policy and practice, 8*(2), 96-108.

Wilton, R. (2017). After Snowden–the evolving landscape of privacy and technology. *Journal of Information, Communication and Ethics in Society.*

Winkler, T. (2011). Vertrauenswürdige Videoüberwachung. *Datenschutz und Datensicherheit-DuD, 35*(11), 797-801.

Wittgenstein, L. (1953). *Philosophical investigations*: Blackwell Publishing.

WooChul, C., & JoonYeop, N. (2017). *Relative importance for crime prevention technologies as part of smart city based on spatial information.* Paper presented at the Smart City Symposium Prague (SCSP), 2017.

Woods, E., & Goldstein, N. (2014). Smart Technologies and Infrastructure for Energy, Water, Transportation, Buildings, and Government: Business Drivers, City and Supplier Profiles, Market Analysis, and Forecasts. *Boulder, CO: Navigant Research.*

Woolgar, S., & Lezaun, J. (2013). The wrong bin bag: A turn to ontology in science and technology studies? *Social studies of science, 43*(3), 321-340.

Wu, C., Zhu, Q., Zhang, Y., Du, Z., Ye, X., Qin, H., & Zhou, Y. (2017). A NOSQL–SQL hybrid organization and management approach for real-time geospatial data: A case study of public security video surveillance. *ISPRS International Journal of Geo-Information, 6*(1), 21.

Wu, D., Zheng, S.-J., Zhang, X.-P., Yuan, C.-A., Cheng, F., Zhao, Y., . . . Huang, D.-S. (2019). Deep learning-based methods for person re-identification: A comprehensive review. *Neurocomputing, 337*, 354-371.

Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology, 71*(4), 485-490.

Wurtzbacher, J. (2008). Urbane Sicherheit und Partizipation. *Stellenwert und Funktion bürgerschaftlicher Beteiligung an kommunaler Kriminalprävention. Wiesbaden.*

Xiong, M., Chen, D., Chen, J., Chen, J., Shi, B., Liang, C., & Hu, R. (2017). Person re-identification with multiple similarity probabilities using deep metric learning for efficient smart security applications. *Journal of Parallel and Distributed Computing.*

Xu, Z., Mei, L., Liu, Y., Hu, C., & Chen, L. (2016). Semantic enhanced cloud environment for surveillance data management using video structural description. *Computing, 98*(1-2), 35-54.

Yang, K., Zhang, K., Ren, J., & Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. *IEEE communications magazine, 53*(8), 75-81.

Yang, Z., Mahajan, D., Ghadiyaram, D., Nevatia, R., & Ramanathan, V. (2019). *Activity driven weakly supervised object detection.* Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.

Yavuz, N., & Welch, E. W. (2010). Addressing fear of crime in public space: Gender differences in reaction to safety measures in train transit. *Urban Studies, 47*(12), 2491-2515.

Yesberg, J. A., Bradford, B., & Dawson, P. (2020). An experimental study of responses to armed police in Great Britain. *Journal of experimental criminology*, 1-13.

Yoo, S. (2017). Songdo: The hype and decline of world's first smart city *Sustainable Cities in Asia* (pp. 146-160): Routledge.

Zenz, A., & Leibold, J. (2020). Securitizing Xinjiang: Police recruitment, informal policing and ethnic minority co-optation. *The China Quarterly, 242*, 324-348.

Zevitz, R. G., & Rettammel, R. J. (1990). Elderly attitudes about police service. *Am. J. Police, 9*, 25.

Zhang, F., Wan, M., Yang, G., & Yang, Z. (2017a). *Background modeling from surveillance video via transformed L 1 function.* Paper presented at the 2017 International Smart Cities Conference (ISC2).

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017b). Security and privacy in smart city applications: Challenges and solutions. *IEEE communications magazine, 55*(1), 122-129.

Zhang, S., & Yu, H. (2018). Person Re-Identification by Multi-Camera Networks for Internet of Things in Smart Cities. *IEEE Access, 6*, 76111-76117.

Zhang, T., Chowdhery, A., Bahl, P. V., Jamieson, K., & Banerjee, S. (2015). *The design and implementation of a wireless video surveillance system.* Paper presented at the Proceedings of the 21st Annual International Conference on Mobile Computing and Networking.

Zhao, G., Ma, H., Sun, Y., Luo, H., & Mao, X. (2011). *Enhanced surveillance platform with low-power wireless audio sensor networks.* Paper presented at the 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks.

Zheng, Y., Sheng, H., Zhang, B., Zhang, J., & Xiong, Z. (2015). Weight-based sparse coding for multi-shot person re-identification. *Science China Information Sciences, 58*(10), 1-15.

Zhou, W., Saha, D., & Rangarajan, S. (2015). *A system architecture to aggregate video surveillance data in Smart Cities.* Paper presented at the 2015 IEEE Global Communications Conference (GLOBECOM).

Zhu, S., Li, D., & Feng, H. (2019). Is smart city resilient? Evidence from China. *Sustainable cities and society*, 101636.

Zingoni, A., Diani, M., & Corsini, G. (2017). A flexible algorithm for detecting challenging moving objects in real-time within IR video sequences. *Remote Sensing, 9*(11), 1128.

Zurawski, N., & Czerwinski, S. (2007). Sie sind doch auch für Videoüberwachung, oder...?" Warum Umfragen zu Kameraüberwachung nicht unbedingt eine Antwort auf das geben, was sie eigentlich wissen wollen. *Der Kriminalist, 39*, 214-220.

Zygiaris, S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of the knowledge economy, 4*(2), 217-231.

APPENDIX 1: Interview Questions

Overall aim and objectives

1. Realistic scenarios

- Are you aware of any smart city initiatives?
- What are possible deployment scenarios in London?
- Which alternatives are most feasible? — financially, ethically, practically…?

2. The current process

- How long does it take to deploy a new technology?
- What things are primarily considered in the process?
- What kinds of consultations are being held before?
- Are issues of ethics and social acceptability considered before?
- I know that many councils now try to buy new security technologies in bulk/together, has this changed the evaluation and consultation process in any way?

3. Suggestions for the future

- Where do you see room for improving the current consultation processes?
- (This is kind of inevitable.) In an ideal world what would smart security systems look like?