UiO : Faculty of Law
University of Oslo

Surveillance and human rights in the digital age

A case study of China's social credit system.

Candidate number: 8012

Submission deadline: May 15, 2019

Number of words: 19.937

Acknowledgements

First, I would like to thank my supervisor Peris S. Jones for his patience, encouragement, enthusiasm and valuable feedback along the way. I also want to thank staff and students at the Norwegian Centre for Human Rights for two challenging and inspiring years. Thank you to my family, and especially my father for reading through countless essays during all of my years as a student. I am very grateful to the Fritt Ord Foundation for believing in my research and granting me a scholarship. Thank you to everyone who participated in the Master's seminar at the Asian Network at UiO, and particularly Henrik Nykvist for recommending interesting literature and providing valuable input to my research design. Finally, thank you Rune, for teaching me all things tech and always lifting my spirits.

Abstract

The social credit system aims to rank Chinese citizens, companies, organizations and government entities by their trustworthiness. Trustworthiness is awarded as credit points based on compliance with legal, moral, and professional norms and standards. The accumulated credit score can affect one's possibilities in life, and the system aims to encourage trustworthiness by offering advantages to those with a high score, and similarly punish untrustworthiness by enforcing sanctions upon those with a lower score. This master's thesis in human rights addresses a few key issues in the nexus of surveillance, technological development and human rights. A case study of China's social credit system serves as an illustration of how the relationship between human rights and surveillance is transformed through technological development. In particular, the thesis examines the rights to privacy and non-discrimination, in relation to both surveillance, technological development, and the social credit system. Big data and Artificial Intelligence are particularly examined from a human rights perspective, and the thesis finds that these technologies substantially affect human rights challenges posed by surveillance. Further, the thesis seeks to understand the cultural and historical context within which the SCS has been implemented. The thesis finds that although the social credit system might be unique in its "gamification" of social life, developments in surveillance technology suggest that trends in the social credit system are present in several other parts of the world. As several researchers have noted high approval rates of the social credit system among Chinese citizens, this thesis attempts to explore the credit system in a nuanced and unbiased way, while considering which human rights implications it may have.

Table of contents

1 Introduction

The fourth industrial revolution is changing how we conduct our every-day lives.[1] Smart technology can help you keep track of the content of your fridge, turn the heat on in your apartment before you come home from work, or register your license plate so you do not have to bother with physically paying for parking. Companies can use artificial intelligence to recruit new employees, health researchers can use big data to find new patterns on diseases, and some researchers have even used big data generated from Twitter messages to predict people's moods.[2] Societies are becoming *datafied*, and plenty of new services make completing our everyday chores and work tasks slightly more convenient. Smart cities are providing efficient ways of transportation and making it easier to get around. However, these new technologies can also pose serious risks to human rights and freedoms. Smart devices provide data that can be used for purposes such as profiling and behavioral predictions. This means that our daily activities are quantified into data that could be traced back to us, and smart cities can become surveillance cities.[3] Smart technology and artificial intelligence depend on data to develop and learn. The collection of this data usually involves some form of surveillance.[4]

In 2014, the Chinese government launched its plan for the *social credit system* (SCS), a new policy that will be implemented by 2020.[5] The SCS will rank all Chinese citizens by a rating scheme, which will not only include financial credit as is normal in several liberal democracies today, but also social credit based on morality and other social indicators. This topic has received wide but varied attention in media and academia. The SCS has been depicted as an Orwellian nightmare - a dystopian foreshadowing of an all-seeing technological surveillance state, and as a threat to democracies worldwide as China rises to global hegemony and Chinese investments are omnipresent.[6] The SCS is still a rather mysterious and unknown subject, particularly regarding its implications for human rights. Understanding the SCS and its scope, and the potential consequences of an all-seeing technological surveillance and social control system, can illustrate potential pitfalls of rapid technological development. In order for the SCS to work, the Chinese government must engage in large-scale surveillance of its

[1] Schwab, *The Fourth Industrial Revolution*.

[2] Mayer-Schönberger, Cukier, *Big Data*, 15.

[3] Sætnan et al., "The Politics of Big Data," 7.

[4] Ibid.

[5] State Council, "Planning Outline."

[6] E.g. *The Telegraph*, "Black Mirror is coming true in China."

citizens. Surveillance affects several human rights, most notably the right to privacy, but also in several cases it can affect rights related to equality and non-discrimination, and other human rights such as the freedoms of speech and assembly. Technological development enable companies and governments to utilize surveillance in entirely new ways, and there are examples of peer-to-peer surveillance taking place as well.[7]

Using a human rights-based approach, this thesis seeks to understand how surveillance challenges human rights, and further how these human rights challenges are transformed with technological development. Finally, a case study of the Chinese social credit system serves as an illustration of how the relationship between human rights and surveillance is transformed through new technology. Based on the situations described above, this thesis seeks to address the following two research questions:

1. Which challenges does surveillance pose to the rights to privacy and non-discrimination?
2. How are these challenges changed by new technologies?

Furthermore, the thesis studies surveillance theory and developments in technology in order to understand China's SCS. The credit system can also help illustrate the development in human rights challenges that new surveillance technology brings. Due to the scope of the thesis, research question 1 does not attempt to assess *all* the human rights that surveillance challenges, but rather *how* surveillance challenges the right to privacy and principle of non-discrimination. The right to privacy is probably the right that is most directly linked to surveillance. Further, reports of the SCS thus far indicate that the system will have an impact on the principle of non-discrimination. Therefore, I will return to these human rights throughout the thesis. Other rights that may be affected by surveillance which are not assessed in this thesis include the right to peaceful assembly, freedom of expression and the subsequent right to find information, the right to health, group rights, and the right to family life.[8] Similarly, assessing the broad range of recent technological developments is outside of the scope of the thesis as well as my knowledge. The term "new technologies" might not sit well with computer scientists, but for this thesis I will nevertheless deploy the term, while specifically assessing artificial intelligence and big data from a human rights perspective.

[7] Creemers, "Cyber China."

[8] OHCHR, "Privacy in the Digital Age," 14.

1.1 Methodology

This thesis is the result of a qualitative research process, and consists of two main parts. In the first part, Chapter 2 presents the theoretical underpinning of my thesis through introducing surveillance studies and linking surveillance to human rights. Further, chapter 3 presents a discussion on how human rights challenges posed by surveillance are transformed by developments in technology. For this first part, I have mainly carried out a human rights-based textual analysis of different theories, both through primary and secondary literature. The goal has not been to choose a single theory of surveillance that might best work to explain the topic of interest, but rather to understand surveillance as a theoretical concept in order to better map out a few key human rights challenges. The theoretical foundation serves as a framework for the second part of the thesis.

Through chapter 4, second main part of the thesis seeks to understand the Chinese SCS in light of these human rights challenges. To analyze the SCS, I have carried out a small case study. The theoretical focus and my interest in studying the SCS as an illustration to changes in the human rights challenges posed by surveillance has led me to choose an ideographic and theory-guided case study as my research design. It is difficult to obtain clear and non-biased data on the social credit system, both because it has not yet been fully implemented, and because of the lack of transparency and information in a non-democratic regime like China. Therefore, the case study is mainly based on secondary literature and unofficial translations of public statements and regulations. I have selected a few main paragraphs from the Chinese government's Planning Outline on the SCS,[9] and consulted with an official translator to make sure that I have understood them correctly.[10]

I started the process of research with a thorough literature review. I performed several searches in databases, mainly Oria[11] and JSTOR,[12] and used the bibliographies of articles and books as points of departure. Further, I consulted a number of professors and experts on the different sub-topics of my thesis, including participating in a Master's seminar organized by the Asian Network at the University of Oslo.[13] The literature review included literature on surveillance theory, on the rights to privacy and non-discrimination, new technologies, and

[9] State Council, "Planning Outline."
[10] Christensen, "Lær kinesisk AS".
[11] Oria.
[12] JSTOR.
[13] UiO, "Network for Asian Studies".

the SCS. Through the literature review, I was able to narrow down my research questions. I have chosen to carry out a case study based on qualitative desktop research, as it can be helpful in shedding light on a theoretical concept.[14]

1.1.1 Multidisciplinary human rights-based approach

This thesis is multidisciplinary and includes elements of several different methodological disciplines. To link the topics to a theoretical framework, I carried out a literature review using textual analysis, and examined theories from different angles, both generally and in the Chinese context. This is in line with the law-in-context method within the comparative legal methodologies. The method highlights the idea that law is a social phenomenon created within the context of society and culture and cannot be seen as an extra-societal and objective, non-social construct.[15] The literature review also includes UN documents, both legal and non-legal. Hence, the study also uses legal method, specifically the doctrinal method to unveil the legal scope and application of human rights, in particular as relates to rights to privacy and non-discrimination. Further, through analysis of government statements and policy, I have also applied elements of policy analysis as a methodology.[16]

The overarching topic of how new technologies may pose both challenges and opportunities for human rights places the thesis into the multidisciplinary fields of digital humanities. Digital humanists combine the fundamental humanist question of what it means to be human with the study of technology and digital life, in order to study what life is like in the information age.[17] Within this field, essential questions include what kind of information societies we want to build, and what our "human project" is for the digital age.[18] This thesis seeks to understand the nexus between human rights, surveillance, and new technologies, and as such assesses challenges and opportunities within information societies. A human rights-based approach to technological development implies assessing which human rights implications technologies have, and how we can incorporate rights and freedoms into our technology.

---

[14] Yin, *Case Study Research*, 40.

[15] Focarelli, *International Law as Social Construct*, 33.

[16] Harris, "Policy Analysis."

[17] Davidson, Savonick, "Digital Humanities," 160.

[18] Floridi, "Soft ethics," 2.

The benefits of multidisciplinary research are many. A flexible methodology that includes several different sources of data and methods enables a wholesome and broad study of a social phenomenon such as the SCS. Surveillance is both a social and technical concept, and the developments of new technologies are not merely technical matters – they most definitely also affect societies and our daily lives. As such, both the developments in technology and the SCS are worth studying in a multidisciplinary human rights framework. Developments in technology affect issues that range from mundane topics like dating, to large-impact development projects or governance. Understanding the broad impact of technology, both in practice and in theory, arguably benefits from a multi-disciplinary approach.[19]

1.1.2 Case study

A case study can be defined as "an attempt to understand and interpret a spatially and temporally bounded set of events".[20] Levy constructs a typology of four ideal types of case studies: ideographic case studies, hypothesis generating case studies, hypothesis testing case studies, and plausibility probes. This thesis mainly includes element of the ideographic, theory-guided case study, but as Levy points out, the different types are ideal types, and in practice a case study may include characteristics of several of the ideal types.[21] The goal of an ideographic case study is to construe, explain or describe a case in itself. It is not a means to developing a higher, generalizable theory. Levy identifies two types of ideographic case studies: inductive case studies and theory-guided case studies. This thesis falls within the scope of the latter type. A theory-guided case study is structured by a theoretical framework, and seeks to explain or construe an historical phenomenon. It is useful in illustrating theories, which in many ways is what I have set out to do.[22] The theory thus helps us interpret the empirical data and understand a specific case. Hence, this thesis should not be read as an effort to "test" a theory or investigate how well a theory explains a phenomenon.

Gerring argues that country-specific case studies should be able to illustrate a broader context or development.[23] Although my findings are not statistically generalizable and the

[19] Cath, "Governing AI,"ibid.
[20] Levy, "Case Studies," 2.
[21] Ibid., 3.
[22] Ibid., 5.
[23] Gerring, *Case Study Research*, 4.

case does not serve as a sample of a broader concept, it is interesting to examine for many reasons. Firstly, the SCS clearly illustrates new human rights challenges that can arise with developments in technologies. As such, it can help inform governments and technology developers of human rights issues that need to be addressed when introducing new technology, and how to build human rights and freedoms into technology. Secondly, the SCS is often sensationalized and portrayed as something completely new and unique in most newspaper articles, but my case study shows that this is not necessarily the case. Although the Chinese government's extensive use of new technologies and data mining for social and behavioral control might be unique per se, many of the issues that it poses are familiar, both in the Chinese context and in other parts of the world. The thought of collecting data for social control or for producing model citizens is also not a new concept in Chinese society. New technologies, however, have the possibility to augment these challenges in entirely new ways. The SCS in many ways represents a dystopic image of what can happen when we do not regulate the use of data and new technologies. However, we have also seen instances of extensive data collection resembling surveillance performed by both states, large corporations and insurance companies in the West, for instance.[24] Further, several scholars report high approval ratings for the SCS.[25] I will return to these discussions later on in the thesis, but the point here is that the SCS is a relevant case because it may teach us something about how technology can be used and misused, and how human rights challenges evolve with new societal and technological developments.

1.2 External validity and relevance

This section assesses the relevance and external validity of my study, or the degree to which the case can be generalizable to other scenarios. The case study carried out in this thesis is useful to get a sense of how human rights challenges from surveillance and technology may play out in practice. As noted by Solove, many people do not worry about invasive surveillance, as they "have nothing to hide".[26] Others point to a so-called chilling effect of surveillance, where we, perhaps even subconsciously, begin to behave as if we are constantly

[24] E.g. the Facebook/Analytica scandal in 2018: *Wired*, "How Cambridge Analytica Sparked the Great Privacy Awakening."

[25] Kostka, "SCS and Public Opinion".

[26] Solove, ""Nothing to Hide"."

being watched, meaning that (the idea of) surveillance directly affects our behavior.[27] These descriptions somehow point in two different directions: on the one hand, it is business as usual, and surveillance does not affect people's behavior because according to themselves, their behavior is not worth watching (or sanctioning). On the other hand, people will alter their behavior, consciously or subconsciously, because they think they are under constant surveillance and are unwilling to share the range of their actions with whomever is watching.

These two scenarios are similar, however, in their trivialization of privacy; we either do not mind that we are being observed, or we silently consent to changing the way we act in fear of surveillance. If we do recognize that surveillance affects human rights, and that new technologies open up for new and more invasive surveillance practices, it is relevant to study these topics more closely. One might claim that the SCS is an extreme example, a statistical outlier that is not analytically generalizable to other forms of surveillance and social control. However, examples from both corporations and democratic governments show that this is not necessarily the case. The way in which the data is used in the Chinese context with credit scoring and social engineering seems unique, but the collection of vast amounts of data by means of surveillance is hardly uncommon. Hence, although this study is not statistically generalizable, it may be of analytical value to other cases than that of the SCS.[28] Further, as an object of research, it serves as an interesting example of how challenges to human rights evolve with the introduction of new technologies and trends in society.

1.3 Challenges to the research

Researching a current topic is certainly rewarding. Several articles about the SCS have been published as I have conducted my research, and there is clearly an interest in learning more about it. In January, Norwegian state media channel NRK published several articles about the SCS, and attention towards the topic peaked.[29] NRK devoted prime television time to discuss the topic, and professionals from different sectors joined the debate. This widespread attention undoubtedly strengthened my motivation as well. At the same time this also makes it a difficult topic to research. I have had to rely mostly on secondary sources. Given

[27] Stoycheff, "Under Surveillance."

[28] Yin, *Case Study Research*, 40.

[29] *NRK*, "Digitalt diktatur."

the scope and timeline of the thesis, I did not have the possibility to test the research results of other scholars, or carry out fieldwork on my own. This also led me to choose a theoretical angle from which to study the SCS, and the thesis should therefore be seen as a contribution to raise attention to the SCS and how new technologies entail new challenges for human rights. Further, the SCS is far from a unitary, single system. It consists of a large web of systems, across private and public sectors, and on multiple levels of government. Hence, it is not simple to grasp the entirety of the systems, and it has been challenging to select the aspects that may be relevant to the thesis. For this reason, I have attempted to draw out a few main characteristics of the system and how these are viewed by other scholars.

Basing a thesis largely on theoretical and secondary sources means that I must be attentive to selection bias. Historians and other researchers may have analytic biases; hence, their biases can affect the objectivity of my own research. This should guide me as a researcher to openly state any underlying analytical assumptions, and to emphasize the potential weaknesses of my research design.[30] Similarly, the statements from the Chinese government that I have used in my thesis are mostly collected from a database of unofficial translations, and my conversational skills in Chinese are not sufficient to read academic or legal Chinese.[31] Further, there is an obvious obstacle in collecting unbiased information from authoritarian regimes. Another challenge worth mentioning in this regard is that the thesis is written from a Western perspective. Although I have strived to approach the literature and information with an open mind, any researcher should be sensitive to her own cultural bias, mine being a Norwegian background having grown up in an open, liberal democracy. On the other hand, having spent several years in China both as a child and as a student, I have also tried to put my personal connection to Chinese culture and society aside.

As I have argued, a multidisciplinary study of technological developments in general, and the SCS in particular, is judicious for many reasons as technology both affects and is affected by several aspects such as the environment, human life, law, society, etc. I am interested in technological development, but I do not have a technical background. Therefore, a challenge to this research is that I cannot fully grasp how the technologies that I have studied technically work. Future research on these topics will benefit from having a diverse group of scholars with different backgrounds working interdisciplinary to grasp the challenges in a deeper and more meaningful way.

---

[30] Levy, "Case Studies," 9.

[31] "China Law Translate".

To ensure construct validity of my research despite the challenges mentioned above, I have consistently attempted to be critical in my assessments of academic and non-academic contributions to the different topics.[32] Further, I have made sure to identify the sender, and examine the report or paper in light of the person or institution that wrote it. Finally, I have also considered the potential strengths in my own biases, e.g. the advantages in the perspectives that may come from having life experience from two countries with significantly different political regimes and traditions.

[32] Yin, *Case Study Research*, 46-47.

2 Surveillance and challenges for human rights

This chapter examines the concept of surveillance through the theoretical lens of surveillance studies, and assesses how surveillance affects human rights.

2.1 Understanding surveillance

The word surveillance can encompass diverse activities ranging from those of the secret police of the former German Democratic Republic, to employees being required to stamp in at work.[33] These practices differ significantly from one another as objects of research. How can we then understand surveillance in a broader theoretical context? The etymological meaning of surveillance refers to *sur* (from above) and *veillance* (to watch).[34] Lyon and Zureik describe surveillance as "the monitoring and supervision of populations for specific purposes".[35] Surveillance is an integral part of modern bureaucracy and an important tool for institutions that keep complex information about large populations. Lyon argues that being a part of modern society entails being under electronic surveillance. Every time we use a credit card, cross a border, drive a car, etc., information about us and our activities is stored in computers and checked against other known details, such as nationality, place of birth or marital status, thus creating a digital biography.[36] However, surveillance is not only bureaucracy. Surveillance is also a way of ensuring that citizens follow social rules and expectations, and constitutes a form of social control. Conversely, surveillance ensures that we receive salary and welfare services, makes sure elections are free and fair; it can help hinder terrorist attacks and crime as well as allow us easy access to our health data. Surveillance is thus, according to Lyon, both about caring and controlling. Those subjected to surveillance are watched for a purpose, and this purpose might be social control and discipline, but might also be for protecting the subject.[37] In other words, modern surveillance is "not unambiguously good or bad".[38]

---

[33] Galič et al., "Bentham, Deleuze and Beyond," 10.

[34] Ibid.

[35] Lyon, Zureik, *Computers, surveillance, and privacy*, 3.

[36] Lyon, *Electronic Eye*, 4.

[37] David Lyon,"Surveillance theories."

[38] *Electronic Eye*, 5.

Surveillance is complex, and there is a need for a comprehensive approach that does not simply amount surveillance to Orwell's "1987".[39]

The Janus-faced nature of surveillance makes it all the more interesting as an object of research. Galic et al. offer an overview of surveillance studies and they categorize surveillance theories into three phases. The main characteristic of theories belonging to this first phase of surveillance studies is the focus on physical and spatial aspects of power and surveillance. Bentham and Foucault's theories of surveillance belong to this phase.[40] Foucault uses Bentham's panopticon to illustrate disciplinary power. Bentham's (prison) panopticon is a vision of a prison constructed as a circular building where the inspector sits in a tower and sees all prisoners, but the prisoners cannot see each other or the inspector. Prisoners are constantly surveilled and controlled, or at least have the illusion of being constantly monitoried. Foucault claims that this is the organizing principle of modern prisons as well as other state institutions. The construction of the panopticon creates a power imbalance between the inspector and those being monitored, because it allows the few to see the many, while the many cannot see each other. Thus, the panopticon embodies the etymological meaning of surveillance, as a structure for watching subjects from above. Another important feature of the prison panopticon is that it influences the observed subjects indirectly as they will start to behave as if they are constantly being watched.[41] Foucault argues that the disciplinary society leads to norm creation - a "habitualization" of the government's preferred behavior for citizens.[42] Further, the mode of government has shifted from the collective to the individual, where individuals are measured against an objective norm.[43] Foucault's rendition of the panopticon is criticized for being overly simplified, but as an object of study, it has analytical vigor because it is clear and easy to grasp.[44]

The second phase of surveillance studies includes infrastructural surveillance theories dealing with networked and digital surveillance. This entails a shift from institutions to networks, and means that there is a distance to the subjects that are watched, and that surveillance deals more with data than physical persons. These theories represent an alternative to the panoptic view of surveillance. Haggerty and Ericson speak of a surveillant

[39] Ibid., 223.
[40] Galič et al., "Bentham, Deleuze and Beyond," 10.
[41] Ibid., 9.
[42] Foucault, *Discipline and punish*.
[43] Galič et al., "Bentham, Deleuze and Beyond," 17.
[44] Ibid., 15.

assemblage where individuals are decomposed and abstracted into data flows, followed by a reassemblage into "data doubles".[45] Surveillance now covers the entirety of the population, not merely certain marginalized groups as in the prison panopticon, and social control is de-territorialised.[46] Deleuze also argues that there has been a shift from the disciplinary society to a society of control. Surveillance becomes more opaque and abstract as opposed to the physical view of surveiallance in the panoptic theories. A fragmentation of society is coupled with a fragmentation of the individual, creating a divided individual, or *dividual*,[47] where power is now used to control access, and surveillance is driven by a need to tie disparsed systems together. We can speak of *dataveillance* as "the systematic monitoring of people or groups, by means of digital information management systems, in order to regulate or govern their behavior";[48] or as studying people's behavior based on the digital traces that they generate. Further, the Foucaultian focus on closed institutions and spaces is passé and the focus is now on open spaces and distanced, technological control.[49]

This second phase also includes the concept of *surveillance capitalism* which combines concepts such as "dataveillance, access control, social sorting, peer-to-peer surveillance and resistance".[50] These neo-Marxist theories encompass both horizontal and vertical surveillance, across sectors and levels of society, and include both digital and physical modes of surveillance. Zuboff claims that there is no longer a relationship of reciprocity between the consumer and the firm – the capitalistic surveillance infrastructure makes firms dependent on thrid parties such as advertisers.[51] This leads to a power imbalance due to a lack of consent when companies extract data and target advertisement based on personal data to uninformed consumers. Additionally, it is nearly impossible to opt out of the big data scheme, and we are witnessing a commodification of behavior.[52] Lyon argues that surveillance leads to social sorting, where individuals are categorized in groups according to certain characteristica registered through surveillance.[53]

---

[45] Haggerty, Ericson, "The surveillant assemblage," 606.
[46] Galič et al., "Bentham, Deleuze and Beyond," 21.
[47] Deleuze, "Postscript on the societies of control," 5.
[48] Esposti, "When big data meets dataveillance."
[49] Galič et al., "Bentham, Deleuze and Beyond," 23.
[50] Ibid., 9.
[51] Zuboff, "Big other," 75.
[52] Ibid., 79.
[53] Lyon, "Surveillance, Security and Social Sorting," 163.

The third phase of surveillance studies represents hybrid theories or concepts that combine elements from the first two phases. While the first panoptic theories are fairly straight-forward, the second phase represents a shift, with a focus on new technologies and the dispersity of data. However, the second-phase theories are not technology-neutral, meaning that they will need to change according to technological development and specific cases.[54] The third-phase theories are less technology-dependant. Lyon argues that we are all both watching and being watched through social media, government surveillance, and new technologies.[55] Surveillance is now a part of every-day life and not limited to institutions such as prisons. From entertainment to education, variations of the panopticon are present in different formats. This "panopticommodity", as Lyon frames it, is just a modern way of forming docile populations, just as Bentham argues with the prison panopticon.[56] Within this phase, scholars also focus on the possible positive effects of surveillance, and the concept of participatory surveillance through social networking sites. As Albrecthslund argues, users of social networking channels participate in self-surveillance, and we should no longer have a "hierarchical understanding of surveillance". This has the potential to empower rather than violate the user.[57] A counter-argument to Albrechtslund's thesis of participatory surveillance, however, is that although users consent to and actively engage in being watched by other users, they also leave vast amounts of data to be traced in the background by commercial third parties.[58] In summary, the third phase of surveillance theories represents a spiderweb of surveillance, in which surveillance crosses sectors and hierarchies, and where there is room for participatory surveillance including a focus on possible positive effects of surveillance.

Although the landscape of surveillance theories is diverse, there are still a few key notions that can assist us in studying concrete societal phenomena in light of surveillance theory. Based on the theoretical foundations laid out in this chapter, this thesis will particularly study three fundamental dimensions or axes of surveillance practices: First, it is interesting to study the actors involved, and the relationship between those being observed, and those performing the surveillance. In this regard, we may look closer at their hierchical relationship and their motivations, such as the reasons for the surveillance, as well as the subjects' awareness of the surveillance and possible acts of resistance. Second, we can assess

[54] Galič et al., "Bentham, Deleuze and Beyond," 30.

[55] Lyon, "Surveillance theories," 4.

[56] *Surveillance studies*, 4.

[57] Albrechtslund, "Online social networking."

[58] Galič et al., "Bentham, Deleuze and Beyond," 31.

the modes and degree of surveillance, including which tools or technologies the surveillor utilizes, and whether surveillance is overt or covert. Third, we may also assess surveillance against existing regulations and legal limitations. Taken together, these three axes can help us distinguish different types of surveillance, and gain a deeper understanding of trends and nuances in surveillance. A prison guard watching over prisoners arguably constitutes a different type of surveillance than companies monitoring potential customers' Google search history. The ever-increasing role of new technologies and digital surveillance, as well as the inclusion of surveillance as a tool in the private sector and not just between the government and the citizen, calls for an interdisciplinary and holistic approach to surveillance.

This first section has discussed how we can understand surveillance as a concept and practice. The following section will assess *affects* of surveillance, in particular how surveillance affects the human rights to privacy and non-discrimination.

2.2 Surveillance and human rights

Surveillance can affect the fulfilment of several human rights. Some positively, e.g. the right to life and several social and economic rights. We may be willing to accept surveillance in terms of the government collecting health data if this will lead to better diagnosing and individually tailored medicine, or inform the government on trends that might require large-scale preventive health policies, for instance. Arguably, the government depends on information to make informed decisions that affect the lives and security of citizens, and thus the government's success in fulfilling its human rights obligations. If one is under the impression that one has nothing to hide, it might be easy to accept surveillance as a necessary means for a safe and prosperous society. On the other hand, surveillance is problematic from a human rights point of view in many ways. The following sections will briefly examine the human rights to privacy and the principle of non-discrimination in relation to surveillance.

2.2.1 Surveillance and the right to privacy

The most obvious and direct example of a human right affected by surveillance is probably the right to privacy. Westin defines privacy as "the claim of individuals, groups, or

institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[59] The right to privacy is recognized in both international, regional and national legislations, and as argued by the High Commissioner for Human Rights, "there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice".[60] The right to privacy is stipulated in article 12 of the Universal Declaration of Human Rights (UDHR),[61] and in article 17 of the International Covenant on Civil and Political Rights (ICCPR). Article 17 ICCPR states that every individual has a right to privacy, and "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation".[62] The Human Rights Committee notes that the word "arbitrary" requires that even legal interferences must be particular to the circumstances, reasonable in scope, and follow "the provisions, aims and objectives of the Covenant".[63] Further, under article 17(2) of the ICCPR, individuals also have "the right to the protection of the law against such interference or attacks".[64]

Under international human rights law, states have an obligation to respect, protect and fulfil the human rights of their citizens.[65] The state should respect its citizens' privacy by refraining from interfering with their private lives, and refraining from attacking or damaging citizens' reputation and honor. The requirement of states to protect citizens' rights implies that states must ensure that third parties do not interfere with citizens' right to privacy. Finally, states must fulfil the right to privacy by making sure that there are adequate safeguards against unlawful interference or abuse of collected information, and that victims of such interference have access to remedy.[66] Obligations under the right to privacy in terms of surveillance require that the state must refrain from engaging in surveillance as long as it is not necessary and within the legal boundaries described above. Secondly, states must also make sure that companies, organizations or other third parties do not engage in surveillance that infring-

[59] Westin, *Privacy and Freedom*, 7.
[60] OCHCHR, "Privacy in the Digital Age," para. 11.
[61] United Nations General Assembly (UNGA), "UDHR."
[62] "ICCPR."
[63] Human Rights Committee, "General Comment No. 16," 4.
[64] "ICCPR," article 17.
[65] de Schutter, *International Human Rights Law*, 280.
[66] Human Rights Committee, "Concluding observations."

es on citizens' privacy. In order to fulfil the right to privacy, states must take administrative and legal measures to combat and reduce infringements on citizens' privacy.

Despite the responsibilities that the right to privacy places on the state, there are also certain conditions that may invoke limitations on the right to privacy. As de Schutter argues, most human rights are more of a relative than absolute character.[67] Three main conditions need to be in place for states to impose limitations on human rights. Firstly, the condition of legality requires that the limitation needs to be prescribed through law. This means that a possible limitation to the right to privacy must comply with regulations in both domestic law and international human rights law. In this regard, it is the state's responsibility to ensure that the laws are publicly accessible. The condition of legality for limitations on the right to privacy is stipulated through derogation provisions in international treaties, such as article 4 in the ICCPR.[68] Article 4 lists a number of rights in the Covenant that a government cannot derogate from, and article 17 (the right to privacy) is not one of them. Hence, according to international law a government can under certain circumstances legitimately derogate from or limit the right to privacy.

Secondly, the condition of legitimacy implies that limitations need to be introduced for legitimate purposes. This means that any data collected through surveillance must be used for legitimate and specific aims, and the laws should be precise. They must specify the circumstances that allow for an interference with a person's privacy, including a specification of "categories of persons who may be placed under surveillance", as well as the duration and procedures of surveillance.[69] Respecting, protecting and fulfilling the right to health and other socio-economic rights can be legitimate aims for which surveillance is used as a means, at least to a certain extent. The safety of a person, and security from external threats like terrorism or other attacks, can also prevail when balanced with other rights. Nevertheless, any information gathered through surveillance needs to be used for the specific purpose it was intended, and the mere existence of a perceived threat does not necessarily legitimize limitations on the right to privacy. Finally, the condition of proportionality involves limiting the interference to what is necessary to fulfil the legitimate and legal aim. Thus, the state must

[67] *International Human Rights Law*, 339.

[68] United Nations General Assembly (UNGA), "ICCPR," 4.

[69] OHCHR, "Privacy in the Digital Age," 28.

make sure that there are adequate safeguards to avoid abuse of any information collected through surveillance.[70] Individuals must also have access to remedy in case of abuse.

If we assess the right to privacy along the three axes of surveillance as mentioned in section 2.1, the right to privacy involves several actors. Firstly, as human rights per se regulate the relationship between states and individuals, the right to privacy arguably also includes these actors. Furthermore, the state's responsibility to protect individuals from third parties intervening with their privacy means that we may also include other actors such as organizations and corporations. Both state- and non-state actors engage in surveillance practices that infringe on individuals' right to privacy. States surveilling companies or organizations thus fall outside the scope of the human right to privacy. Further, different modes of surveillance can have different impacts on the right to privacy. For instance, CCTV cameras that capture everything that happens within a public space can affect the right to privacy of many people, whereas monitoring a small group of people with seemingly suspicious characteristics affects fewer people, but perhaps constitutes a graver violation of their right to privacy. The former also represents a more overt surveillance practice, while the latter will usually be covert.[71] Laws regulating the right to privacy are stipulated in both international, regional and national legislations, and under certain conditions, the state can limit the right to privacy.[72] However, there are also grey areas within the scope of the right to privacy. Notably, new technologies pose challenges and new ways of consenting to the collection of data. As technology often develops faster than law in democratic countries, regulating new surveillance practices poses a challenge to the legal dimension of privacy and surveillance.[73]

Surveillance directly affects the right to privacy because gathering information is the core practice of surveillance. Engaging in surveillance, either through visible CCTV cameras or through covertly monitoring e-mail correspondence, is in itself an infringement on the right to privacy. These limitations may be legitimate under international law, yet they do constitute practices that in one way or another diminish the scope of the right to privacy. Further, surveillance by companies or other third parties also affects the right to privacy, and it is the state's obligation to ensure that unlawful surveillance does not happen. This last provision is tricky, as citizens often willingly accept a form of surveillance as part of access to different

[70] Human Rights Committee, "Concluding observations."

[71] Galič et al., "Bentham, Deleuze and Beyond," 30.

[72] E.g. article 17, United Nations General Assembly (UNGA), "ICCPR."

[73] Nemitz, "Constitutional Democracy and Technology," 9.

networks such as social media, and freely provide information that becomes the property of a company once the user hits "publish". I will return to these particular challenges in chapter 3 on challenges to human rights in the digital age.[74]

Surveillance also affects a number of other human rights. Further, it has been argued that the right to privacy is a necessary pre-condition for several other human rights, and even a "gatekeeper to the full exercise and enjoyment of all other human rights".[75] The following section will examine how surveillance challenges the principle of non-discrimination.

2.2.2 Surveillance and non-discrimination

Rights to non-discrimination and equality are central features in several international human rights documents, including through UDHR article 7, and ICCPR articles 2 and 26.[76] Non-discrimination is included in several other articles in international human rights treaties with reference to other rights, i.e. that there should be no discrimination in the granting of- or access to the rights set forth in a convention. It is also a defining characteristic in conventions such as the Convention on the Elimination of All Forms of Discrimination Against Women.[77] Many have also argued that the right to equality before the law is customary international law.[78] There is no definition of discrimination in the ICCPR. The Human Rights Committee denotes non-discrimination as:

"[…] any distinction, exclusion, restriction or preference which is based on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms"[79]

[74] Matzner, "Surveillance as a critical paradigm for Big Data?," 73.
[75] McGregor et al., "Submission to OHCHR," 8.
[76] United Nations General Assembly (UNGA), "UDHR.", "ICCPR."
[77] E.g. article 2, "ICESCR."; "CEDAW."
[78] E.g. *Vice-President Ammoun's separate opinion*, 64.
[79] Human Rights Committee, "General Comment No. 18," 7.

General comment 18 further states that differential treatment can meet the requirement of non-discrimination, as long as there are reasonable and objective criteria, and that the measures are taken to pursue an aim that is "legitimate under the Covenant".[80]

States must respect the rights to equality and non-discrimination by refraining from enacting discriminatory legislation, programs and policy, and refraining from discriminatory and arbitrary law enforcement or other public operations. Further, states are obligated to protect the rights by ensuring that third parties such as businesses do not discriminate citizens. Finally, states must fulfil the right to non-discrimination by promoting equality through policy, laws, and programs, including combating structural discrimination and other instances of groups being permanently disadvantaged, and ensuring access to an effective remedy.[81]

Limitations to non-discrimination need to meet the conditions of legality, legitimacy, and proportionality.[82] Article 4 ICCPR does not list article 2 or article 26 as non-derogable rights. As such, it is possible that states can legally place limitations on the right to non-discrimination. Further, the limitations placed on the right to non-discrimination must be for a legitimate aim. Thus, potentially discriminatory surveillance practices must be for specific and legitimate purposes, and laws must precisely specify the conditions under which surveillance practices can part from the principle of non-discrimination. This also implies that law enforcement cannot apply laws and public decisions arbitrarily.[83] In a judgement passed by the UK House of Lords regarding British airport immigration officers' discriminatory screening practices directed at Roma people, the judges noted that the intentions of the officers were of significance in the decision. Roma people were "simply because they were Roma" routinely subjected to suspicion and intensive questioning. Given the political context of increasing numbers of asylum seekers from "one comparatively easily identifiable racial or ethnic group", the operation would be hard to set up without discrimination.[84] In this case it was concluded that the operation was "systematically discriminating" based on its use of ethnic profiling as a criterion for law-enforcement, and incompatible with both domestic and international law, including customary international law.[85] Lastly, the condition of proportionality requires that discriminatory surveillance must be limited to what is necessary in fulfilling the

[80] Ibid., 13.

[81] de Schutter, *International Human Rights Law*, 647, 701.

[82] Ibid., 339.

[83] *Robert W. Gauthier v. Canada*, 14.

[84] *International Human Rights Law*, 665.

[85] *R v. Immigration Officer*, para. 97-98.

legal and legitimate aims of the surveillance. This means that any discriminatory surveillance practice must be proportionate, and there must be safeguards to avoid abuse and further discrimination.

Surveillance can affect the right to non-discrimination in different ways, and the relationship between surveillance and non-discrimination is not necessarily easy to construe. Surveillance can be discriminatory in its primary stage through its methods for collecting data, and secondarily through how the data is analyzed and used. As was shown in the airport case above, surveillance can be directly and systematically discriminatory. On the other hand, surveillance can be remarkably equal, especially with new technologies that can allow surveillance to be all-encompassing, and hence not necessarily single out certain groups.[86] However, although this type of surveillance may not single out certain ethnic groups, for example, we may see the rise of new, discriminatory grouping systems based on other seemingly arbitrary characteristics. Big data generation and analysis is not free from selection bias, and we should not assume that data is objective and "raw". Further, big data may lead to a series of spurious correlations.[87] As I will show in the next chapter, big data analysis yields correlations but not causality, which in itself is not a problem as long as those interpreting the correlations are able to identify them as such.

If we revisit the three axes for studying surveillance, questions of equality and non-discrimination address the discussion on actors of surveillance and their hierarchical relationship. The nature and intentions of the institution performing the surveillance is likely to affect the degree to which surveillance is discriminatory. Surveillance data used to improve medication for a group of patients arguably constitutes a different case than security officers systematically monitoring an ethnic group, for instance. Both practices constitute surveillance, but the intentions and purposes are significantly different, and this also affects the degree to which the principle of non-discrimination is affected. Further, there is usually a power imbalance between the actors involved in surveillance. The state or corporation performing the surveillance must be vigilant not to use this power for discriminatory practices. If surveillance targets specific groups, the institution performing the surveillance must select the criteria on which to base the selection of data. Individuals or groups may be particularly vulnerable or subject to systematic discrimination. Those engaging in surveillance should be aware of- and mitigate existing bias. Surveillance often targets groups or individuals with certain character-

[86] Matzner, "Surveillance as a critical paradigm for Big Data?," 72.

[87] Sætnan, "The haystack fallacy," 29.

istics that are thought to correlate with criminal or unfavorable behavior. In cases where surveillance is used to monitor large numbers of people and not necessarily targeted at specific groups, surveillance can affect non-discrimination indirectly through the criteria later used to scrutinize data.[88]

The modes of surveillance can also have an impact on the degree to which surveillance practices are discriminatory. As mentioned, selection criteria for surveillance is key to determine whether the practice is compatible with human rights. Further, whether the practices are overt or covert affects the power balance between the actors involved in surveillance. If an operation is covert and those that are subject to surveillance are unaware that they are being monitored, the operation may be discriminatory, as the subjects do not have information or the possibility to opt out. If the surveillance practice targets a certain group, the practice may infringe on group members' right to equality before the law.[89] Collecting data from some, but not all citizens means that they will not be equal in a courtroom. Interestingly, the modes of surveillance affect non-discrimination in a different way than they affect the right to privacy. Setting up CCTV cameras that monitor the activity that happens within a public space, for instance, is *less* discriminating than monitoring one specific group based on seemingly suspicious characteristics. Surveillance can encompass large segments of the population, and operations do not necessarily need to profile or target specific groups. Thus, it can be possible to collect vast amounts of data without harming the principle of non-discrimination. Again, the question becomes more challenging when we look at how data then is selected for scrutiny, and the purposes for which the information is used.

Surveillance has evolved into a wide variety of practices that exceed the analytical limits of the prison panopticon. This chapter has outlined a few key challenges for the rights to privacy and the principle of non-discrimination. The following chapter seeks to assess how these challenges change with technological development.

[88] Gandy Jr., "Data Mining."

[89] Matzner, "Surveillance as a critical paradigm for Big Data?," 73.

3 Surveillance and human rights in the digital age

This chapter briefly examines some new technologies, particularly artificial intelligence (AI) and big data, and assesses how they might influence the challenges to privacy and non-discrimination highlighted in chapter 2. According to Kranzberg's *First Law of Technology*, "[t]echnology is neither good nor bad; nor is it neutral".[90] Humans shape technologies, but technologies also in many ways shape us. Technology can be used and misused, and the debate should be more nuanced than a dichotomy of tech-optimism versus tech-dystopia. New technologies can improve human rights situations in several ways.[91] However, there are also examples of the questionable consequences of placing advanced technology in the wrong hands. In 2019, it was reported that the Saudi government had launched the app *Absher*. This app enables Saudi men to control women, e.g. by restricting their possibility to use their passport and mobile phone, or by enacting a service that sends a text message to men if their wives are close to an airport.[92] This exemplifies how a government cleverly uses technology to provide an efficient tool for pre-existing practices of social control. Further, *Absher* shows that technology can foster peer-to-peer surveillance, and not simply government-citizen surveillance. Although this particular app does not change the underlying causes of women's rights abuses in Saudi Arabia, it certainly contributes to shrinking women's realm of freedom by providing a more convenient and effective control mechanism, thus affecting fundamental rights such as the right to privacy, freedom of movement and association, and the principle of non-discrimination. The next few sections assess how new technologies, particularly artificial intelligence and big data, influence human rights issues posed by surveillance.

3.1 Artificial intelligence (AI) and big data

AI denotes the ability of machines to make predictions, decisions, and solve tasks based on data and algorithms.[93] Several complex tasks are already delegated to AI systems, such as illness diagnosis, financial transactions and granting parole. AI development requires

[90] Kranzberg, "Kranzberg's Laws."

[91] E.g. the *Cancer Moonshot* collaboration between the Norwegian Cancer Cluster and Lawrence Livermore National Laboratory in California, where high-performance computing in California is used to analyze health data from Norway for individually tailored treatment to patients with cervical cancer.

[92] *Aftenposten*, "Kontroll over kvinnene."

[93] Bolter, "AI," 1.

large amounts of data, often *big data*.[94] Big data is a method of prediction, of showing patterns and correlations based on large amounts of information, offering new insights to different phenomena. As such, big data is not necessarily new as a concept. Statistics, intelligence and other disciplines have "always" set out to collect information, and codified and organized them in large data sets.[95] A few traits separate big data from traditional statistics. A key idea is that new technologies allow data to "tell us what to look for", instead of having to look for something in the data.[96] Further, big data is special in its scale and velocity, producing insights in or near real-time, without the natural lag of other forms of data collection. For example, in 2009, Google's systems could predict the outbreak of the H1N1 virus before the government, as people immediately googled their symptoms, but often waited a week before seeing a doctor.[97] Moreover, big data does not discover causalities, but rather finds correlations.[98] It is flexible, meaning that it is both easy to include a variety of new research areas and easy to scale the size of the data sets. The large quantity of data supposedly allows for a far more detailed picture than what we can see with smaller quantities of data. The data itself can be less precise or exact, because "[w]hat we lose in accuracy at the micro level we gain in insight at the macro level".[99] Big data also uncovers the "latent value" of information through *datafication*, i.e. transforming seemingly irrelevant information into quantifiable data.[100] In summary, we may define big data as "*the collection and aggregation of large masses of […] data and its analysis*".[101]

Researchers have also opposed these arguments in favor of big data. As AI and big data increasingly become a part of both mundane activities like dating and critical services such as health care, it is critical that we assess how these technologies interplay with law and ethics.[102] AI in self-driving cars has brought to life debates on philosophical dilemmas such as the classical schoolbook example of the "trolley problem" where one has to decide which group of people a trolley on the loose should run over. This discussion illustrates that AI has

[94] Sætnan et al., "The Politics of Big Data," 6.
[95] Mayer-Schönberger, Cukier, *Big Data*, 14.
[96] Matzner, "Surveillance as a critical paradigm for Big Data?," 71.
[97] Mayer-Schönberger, Cukier, *Big Data*, 2.
[98] Ibid., 12.
[99] Ibid., 13-14.
[100] Ibid., 15.
[101] Sætnan et al., "The Politics of Big Data," 6.
[102] Cath, "Governing AI."

human bias through biased input data.[103] As argued by Harambam et al., technology is "never an unstoppable or uncontrollable force of nature, but always the product of our making, including the course it may take".[104] As such, it is imperative that technology developers have sufficient knowledge about human rights, just as policymakers need to understand how technology works. Human rights defenders and organizations are increasingly looking into how we can use new technologies to improve human rights situations. Amnesty International has several projects on machine learning and AI in human rights work, including a pilot investigating how AI may be used in court proceedings to give legal advice to poor segments of the population in India.[105] However, this requires "algorithmic fairness" and unbiased data on which to base the legal advice. As we will see, it is difficult to obtain purely unbiased data, and similarly difficult to produce unbiased algorithms by which to process data and develop AI. This again highlights the importance of including human rights and political theory in the AI agenda.[106] The following sections will therefore assess how technologies such as big data and AI change the challenges that surveillance poses to the rights to privacy and non-discrimination.

3.2 The right to privacy in the digital age

In 2013, the United Nations General Assembly adopted the resolution "The right to privacy in the digital age".[107] This resolution calls on states to ensure fulfilment of the right to privacy by reviewing their own practices of data collection and surveillance procedures, and by establishing or maintaining existing mechanisms for ensuring accountability and transparency in relation to the right to privacy. The UN High Commissioner for Human Rights' report on privacy in the digital age highlights that although new communications technologies provide space for citizens to practice their freedom of expression, for human rights defenders to address abuses, and for democratic participation, they also provide governments with an increased capacity to conduct surveillance.[108]

[103] Risse, "Human Rights and AI."
[104] Harambam et al., "Democratizing algorithmic news recommenders," 5.
[105] Risse, "Human Rights and AI," 11.
[106] Ibid., 12.
[107] UNGA, "The Right to Privacy in the Digital Age.."
[108] OHCHR, "Privacy in the Digital Age," 1.

New technologies can reveal intimate details about our lives in much more invasive ways than what has previously been possible through surveillance.[109] Smart devices and the Internet of Things provide data and metadata on countless aspects of our daily lives. This data can later be used for profiling, predicting behavior, or re-identification.[110] Re-identification puts users' anonymity at stake. Data is often anonymized by carefully removing personal identifiers. However, through advanced big data analysis, anonymization can quickly become a false security for users. This was the case in October 2006, when Netflix launched the *Netflix Prize*, a competition where participants competed to improve Netflix's film recommendation system based on rental records from approximately 480,000 subscribers. Computer scientists proved that it was possible to re-identify users based on the released data, and a closeted lesbian mother based in the conservative Midwest of America later sued Netflix in fear of her sexual orientation being revealed on the background of her movie rating records.[111] Further, new technologies such as AI require large amounts of data, and big data has turned seemingly irrelevant information into valuable data. This means that surveillance is no longer "just" an activity performed by the government to keep its citizens under control, or to prevent violence and criminal acts on the street. Surveillance now also includes collecting vast amounts of information about people's daily lives; about their curiosities and interests, based on their search terms; about their sexual identity, based on their Netflix ratings; and about their social network and routines, based on location services.

This *datafication* of seemingly mundane information augments the challenges that surveillance poses to the right to privacy. Datafication is not necessarily in people's consciousness. For instance, most people are likely to think twice before sharing their social security number with private actors online, but we are probably not as worried about the traces we leave elsewhere, as one assumes these traces are irrelevant to analyze.[112] In many cases, this makes sense. As services become digitalized and automated, we should not refrain from using them in fear of leaving traces. It is practically impossible to function in a modern society without leaving any digital traces.[113] Nevertheless, it is noteworthy that datafication is changing the way surveillance works, and the way in which surveillance affects our privacy. The UN Special Rapporteur on the right to privacy has also expressed concern on states' utiliza-

[109] Special Rapporteur on the Right to Privacy, "Submission to OHCHR," 2.

[110] Sætnan et al., "The Politics of Big Data," 7.

[111] Hallinan, Striphas, "The Netflix Prize."

[112] Solove, ""Nothing to Hide"."

[113] Fulton, Kibby, "Millennials and the normalization of surveillance on Facebook."

tion of big data in ways in which limit the right to privacy. He notes that states engage in arbitrary surveillance of citizens, and use big data and health data in a way that infringes "upon the dignity of its citizens based on gender or gender identity and expression".[114]

These practices pave the way for new ways of thinking about the right to privacy, and recent developments in privacy regulations have introduced the concept of *the right to be forgotten*. Article 17 of the EU General Data Protection Regulation (GDPR) stipulates that individuals have a "Right to erasure", and it further notes a number of conditions under which a controller must erase personal data.[115] The question that perhaps remains unanswered is how we can regulate an algorithm. If we revisit Westin's definition of privacy, i.e. that privacy is the claim of people to determine what information about them is communicated to others; it is interesting to note that this definition perhaps does not entirely cover the notion of privacy in the 21st century. Most of us now daily consent to sharing, even "donating", large amounts of our personal data online. Data is often sold on to third parties, and it is questionable whether data subjects actually are aware of what they are consenting to. There is a large body of laws that regulate the collection and use of personal information. Scholars argue that existing legal frameworks do not necessarily cover the entirety of corporations and states' generation, analysis, usage and cross-segmental sharing of data.[116] Further, frameworks may be time-specific, for example targeting the data collection phase, whilst overlooking consecutive data-processing phases. Hence, the requirements of international human rights law contain a "significant implementation gap" and a lack of effective procedural safeguards and oversight. [117]

Big data does not simply scale the challenges to human rights posed by surveillance. As Mayer-Schönberger and Cukier argue, a mere enlargement of the threat would probably mean that existing privacy laws and regulations could still work. They argue that challenges to the right to privacy have been transformed, thus requiring new ways of thinking in terms of privacy laws. Data is now valuable not only for its primary uses, but also for secondary purposes, which potentially "undermines the central role assigned to individuals in current privacy laws".[118] Current privacy regulations require that individuals must be informed about information that is gathered, and which purposes it will be used for, when the information is collected. However, at the time of collection, it is not necessarily clear which big-data analy-

[114] HRC, "Report of the SP," 6.

[115] "EU General Data Protection Regulation (GDPR)."

[116] Schneider, "Bringing the state back in."

[117] McGregor et al., "Submission to OHCHR," 12-15.

[118] Mayer-Schönberger, Cukier, *Big Data*, 153-54.

sis or purpose the information will be used for in the future. Data can be sold on to third parties, and as Matzner argues, data analysis has been decoupled from data generation. This means that data is not necessarily analyzed within the context it was collected. Data is now stored and used for other purposes and future scrutiny. Matzner coins this practice "prospective surveillance" whereby huge troves of data are stored in case they may be used in the future. Thus, as data usage becomes diversified and perceivably unpredictable, "[i]ssues like consent or autonomy become shaky".[119] This highlights the power imbalance that arises because of the lack of consent when companies extract data from uninformed consumers. As Zuboff argues, there is no longer a relationship of reciprocity between the firm and the consumer, and data is shared with third parties.[120] The Special Rapporteur on the Right to Privacy claims that it is "glaringly evident" that existing legal frameworks for protecting privacy have "huge gaps", both at the international and national levels.[121] Data collection is also often a transnational activity, thus creating the need for a separate cyberspace jurisdiction, especially related to surveillance.

The large amounts of collected data can also lead to a stratification of social groups. The American data company Acxiom uses data to categorize subjects according to different codes, such as race and health needs, based on personal data such as voting behavior, criminal records, or gambling habits. By categorizing data subjects, Acxiom offers services to predict people's behavior to corporate clients. There are approximately 70 hierarchically ordered categories, and the bottom 10% are coined "waste". Persons belonging to this category "will never get a good mobile phone contract, private health insurance, or housing credit".[122] These new technologies give an intimate picture of people's lives, and offer much more information "than even a search of a person's home".[123] This shows that collection and analysis of large amounts of data not only affect data subjects' right to privacy, but can also have rather egregious impacts on other rights, such as equality and non-discrimination. The following section will assess how the principle of non-discrimination can be challenged by technological developments in surveillance practices.

---

[119] Matzner, "Surveillance as a critical paradigm for Big Data?," 74.

[120] Zuboff, "Big other," 75.

[121] Special Rapporteur on the Right to Privacy, "Submission to OHCHR," 7.

[122] Schneider, "Bringing the state back in," 138-39.

[123] McGregor et al., "Submission to OHCHR," 3.

3.3 Surveillance and non-discrimination in the digital age

As the Acxiom case shows, data collection can lead to discriminatory practices and new ways of stratifying people in a socio-economic, hierarchical order. Surveillance thus affects the principle of non-discrimination in the way the collected data is analyzed and used. As discussed in chapter 2, surveillance can be discriminatory also in the way in which data is collected. These challenges are still valid with the introduction of new technologies. One may argue that connecting big data to surveillance practices can change the effect that surveillance has on the principle of non-discrimination. For example, using big data analysis to select which passengers to examine more closely at airport security may be less arbitrary than basing these decisions on clothing, ethnicity, or the gut feeling of a security officer. However, data is no guarantee against discriminatory bias. Furthermore, predictions based on big data and AI in security practices will overgeneralize risk. Although the algorithm only estimates a risk factor and does not make a decision, this still leaves open the question of how to make a decision based on a generalized prediction. As argued by Matzner, "*[p]rediction is operationalized bias*". [124] Risk predictions can be useful for large groups of people where one does not need to be correct on each individual case, but they do not work on the individual level. "*Risk estimate for individuals suggest a numerical objectivity"*, but one cannot be "80% terrorist".[125] If we overestimate the accuracy of big data analysis and AI in this regard, we may find ourselves engaging in predictive policing, which will have a direct effect on the right to equality before the law. The principle of presumption of innocence clearly requires more of evidence than a prediction, or else citizens may have to think twice before making the claim that they have nothing to hide.[126]

Violations of the right to privacy often disproportionately affect marginalized groups, thus contributing to strengthening unequal and discriminatory practices. For instance, LGBT+ persons have found new ways to organize and interact on social media, creating spaces for vulnerable people who do not necessarily have the option of discussing issues of their sexual identity with peers. At the same time, states or non-state actors can target these groups and use their personal information, not only interfering with their privacy, but also with the prin-

[124] Matzner, "Grasping the ethics," 40-41.

[125] Ibid.

[126] Cath, "Governing AI."

ciple of non-discrimination.[127] Further, although marginalized groups are often aware of how they are evaluated "by those higher in the social hierarchy", as surveillance methods become more opaque with new and advanced technology, so too the categorization of individuals becomes covert and the information asymmetry deepens.[128] This uncertainty may cause individuals to be extra careful in regards to with whom they associate.[129] This also highlights that Lyon's *social sorting* is still an issue for surveillance in the "digital age", perhaps even more so as data and tools for social sorting and stratification become more efficient.[130]

Big data and AI in surveillance and risk assessments can pose several issues to human rights. An excessive faith in the accuracy of the results and objectivity in data can have discriminatory social consequences. As mentioned, big data allows for less accuracy on the individual level. Hence, predictions based on big data need to be focused on larger trends in society rather than risk assessments on the individual level. Sætnan argues that analytical results frequently have errors and faults that may lead to detrimental consequences of actions taken based on the analysis.[131] Additionally, in many cases it is not necessarily easy to estimate how an algorithm reacts to unknown data. Technologies evolve and learn, and the input data thus decides *how* it will evolve. This means that whichever checks are performed prior to using the algorithm do not necessarily account for failures in the future, and it becomes close to impossible to verify the algorithm's neutrality. Furthermore, even if we could ascertain the neutrality, "algorithms would still produce biased results on biased data".[132] If used unwisely in decision-making under the impression that technologies are both unbiased and transparent, "accountable algorithms might increase the legitimacy" of unjust practices within credit scoring, healthcare benefits, employment, and so on.[133] As an example, an AI tool used to analyze and rate résumés of job applicants at Amazon used an algorithm that was based on data from résumés from job applicants over the past 10 years. As it turned out, most of the résumés belonged to men, reflecting the male dominance of the industry. Accordingly, the algorithm

[127] McGregor et al., "Submission to OHCHR," 5.
[128] Gandy Jr., "Data Mining," 379.
[129] Ibid., 383.
[130] Lyon, "Surveillance, Security and Social Sorting."
[131] Sætnan, "The haystack fallacy," 31.
[132] Matzner, "Grasping the ethics," 39.
[133] Ibid., 41.

consistently rated men higher than women, clearly indicating that the data was not gender-neutral and thus included discriminatory bias.[134]

Algorithms clearly do not automatically produce neutral predictions and correlations. This is of course also the case for humans. However, an important difference is that we have mechanisms that seek to mitigate the bias in human decision-making. These may not be perfect, but they imply an acknowledgement of existing bias, and a commitment to mitigate it, whereas the apparent belief in the neutrality of technology contributes to concealing existing biases.[135] Matzner therefore suggests that we "drop the hope" about algorithmic systems being neutral, transparent and accountable, and accept, state, and mitigate the inherent and potentially discriminatory problems in algorithmic decision-making.[136] Another issue with big data analysis, according to Matzner, is that by discovering "patterns, relations, regularities or rules hitherto unnoticed", it gives us an impression that data includes hidden information that we can extract. This again implies that data is objective or value-neutral and contains information that is not identifiable by humans.[137] Matzner claims that this hope is exaggerated. Conversely, however, this may also be the comparative advantage of big data analysis: it could free us from the traditional and perhaps structurally discriminating categories that we use for surveillance purposes. Big data analysis finds rules, associations and patterns, and is perhaps not interested in outdated categories of characteristics.[138]

3.4 New surveillance technologies, new challenges for human rights?

Through enabling new modes of surveillance, new technologies clearly transform the challenges that surveillance poses to human rights. They may not change the underlying causes of human rights abuses, but new technologies enable existing practices of social control, privacy breaches and discrimination to become more invasive and effective. Further, new practices such as data sharing and "data markets" entail new challenges for the rights to privacy and non-discrimination. Assessing how to mitigate human rights challenges that are posed by new surveillance technologies thus requires an enquiry into not only how data is collected,

[134] *Reuters*, "Amazon scraps secret AI recruiting tool."
[135] "Grasping the ethics," 42.
[136] Ibid., 44.
[137] "Surveillance as a critical paradigm for Big Data?," 72.
[138] Ibid., 75.

but also how data is analyzed and used in consecutive phases, from a human rights perspective. Data sharing means that surveillance is no longer just an act of a superior monitoring an inferior. Data is sold, shared, and used for multiple purposes, often disconnected from the original context within which it was collected. As such, human rights-based approaches to surveillance and technology must consider all the stages of surveillance, and not solely the data collection phase.[139] Haggerty and Ericson's *data double* offers a fruitful theoretical starting point in this regard. Discrimination can occur through all phases of "data mining", and the decoupling of data generation from data analysis further obfuscates the use of data, at the expense of data subjects and their control and ownership over their own personal information.

These developments also require a new enquiry into how the modes and regulations of surveillance are changing. Participatory and "consented" surveillance implies that data subjects often willingly share their personal information, yet perhaps without knowing how their data will be scrutinized and used in the future. In many ways, surveillance is the very essence of big data and AI.[140] As the "business model of the internet", surveillance has now become a tool not just for the government, but also for corporations.[141] The introduction of biometric sensors, finger print recognition, and other (surveillance) innovations means that the risk for undermining several fundamental human rights has increased. Such data is in many cases privately owned and data is becoming an important corporate asset, much resembling Zuboff's "commodification of behavior".[142] An unequal distribution of data leads the large AI companies to become more powerful and develop ever-smarter machines.[143] According to Nemitz, this can be a democratic issue, as governments increasingly become dependent on the private sector to assist them in cyber development, security and policymaking, creating a bigger distance between the legislature and the citizen.[144]

A common criticism from technocrats reads that law develops too slowly and lags behind technology and business models. Nemitz argues that this criticism is misplaced for several reasons. Firstly, there are several examples of technology-neutral law, such as the GDPR, which can be interpreted progressively as technology develops.[145] Secondly, it would be anti-

[139] Ibid., 83.
[140] Lyon, "Surveillance, Snowden, and big data," 2.
[141] Matzner, "Surveillance as a critical paradigm for Big Data?," 68.
[142] Zuboff, "Big other," 79.
[143] Risse, "Human Rights and AI," 12-13.
[144] Nemitz, "Constitutional Democracy and Technology."
[145] Ibid., 9.

democratic to require that law should develop as fast as code, because deliberation, compromise and due process are key democratic values.[146] Nevertheless, technological development and a potential shift in power from governments (and citizens) to corporations certainly do entail new challenges for regulation. Legislation is often inadequate in regulating data sharing across borders, which in the globalized business environment is the norm rather than the exception.[147] On the other hand, strengthening technological skills on behalf of the government does not necessarily mitigate the potential for human rights abuses through surveillance tools. The power of AI can be subtle, and different from our traditional, political understanding of power.

Liu claims that human rights law is inadequate in addressing the human rights issues that AI poses because it is state-centric, while corporations are the threatening actors in this regard.[148] He claims that protections provided by human rights law are circumvented by "tightly integrated technological systems".[149] However, when 37 per cent of the world population according to Freedom House live in societies that are "not free", the state-centric focus of human rights law is arguably still relevant.[150] Recent developments in the business and human rights-nexus might be useful in the quest to govern private AI and big data towards a human rights-friendly application.[151] Nevertheless, this serves to highlight that as corporations grow larger, and tech giants such as Facebook boast billions of users, more than any one country, it is crucial that the rule of law with its necessary checks and balances is imposed to avoid further harm.[152] As Liu argues, AI is often opaque, and individuals are not necessarily aware that their rights have been violated, thus individuals will not bring a claim to court. Further, governments may request to receive data from businesses while requiring that they sign a non-disclosure agreement, thus rendering it illegal for the entity to notify the data subject.[153] Individuals' access to remedy is thus restricted as they are simply unaware of the potentially unlawful practices taking place. This underscores the importance of implementing a legal framework that requires transparency and accountability, as well as notification mechanisms

[146] Ibid.

[147] Special Rapporteur on the Right to Privacy, "Submission to OHCHR," 5.

[148] Liu, "The power structure of AI," 210.

[149] Ibid.

[150] Freedom House, "Freedom in the World 2018."

[151] McCorquodale et al., "Human Rights Due Diligence."

[152] Schneider, "Bringing the state back in," 141.

[153] McGregor et al., "Submission to OHCHR," 32.

between different data actors, so individuals have access to remedy and justice.[154] Access to an effective remedy is also challenged by the use of algorithms in decision-making processes, as individuals often do not have access to the input data and thereby cannot challenge conclusions drawn by algorithms.[155]

A key challenge for human rights is the widespread belief that technology is somehow value-neutral and free from discriminatory bias, and that data can be easily anonymized. As such, the surveillance tools themselves do not necessarily pose the human rights challenges, but rather the lack of knowledge on how they work, leading to a lack of efforts in mitigating discriminatory data bias. This chapter shows that the relationship between surveillance and human rights is transformed significantly by the introduction of new technologies such as big data computing and AI. Although existing legislation can be technology-neutral, some new practices of data analysis and data sharing entail new regulatory challenges, and require new knowledge for lawmakers. Big data and AI enable new and more efficient tools for surveillance, thus augmenting the human rights challenges that surveillance poses. Therefore, it is vital that we put human rights on the technology agenda. Further, it is equally imperative that human rights defenders and organizations, as well as national human rights institutions and others supervising the human rights situations, acknowledge the challenges to the rights to privacy and non-discrimination that technologies might pose in "the digital age". Schneider argues that Big Data can enable the establishment of a "*moral economy*", where people are surveyed and categorized into groups by rating and rank, creating "a metric self" where "people accept their social score as a fair and just assignment of societal place".[156] The next chapter continues this discussion by taking a closer look at China's social credit system.

[154] Ibid.

[155] Ibid., 33.

[156] Schneider, "Bringing the state back in," 137-40.

4 China's social credit system

This thesis has so far provided a theoretical discussion on how surveillance challenges human rights, and how new technologies affect these human rights challenges. The following chapter provides a practical example of how new technologies affect human rights through the social credit system (SCS) in China. As mentioned in section 1.2, the SCS may be an extreme example. Yet, as I have shown, developments in technology pave the way for new and increasingly invasive practices of surveillance across regions and countries, not just in China. Further, the ideas behind the SCS are not necessarily new. There is a long tradition of moral governance in China. The technological system of sticks and carrots itself, however, is rather novel, which also poses a challenge to this thesis. Academic literature on the issue is scarce, but it is evolving rapidly. During the short period within which I have conducted my research, several articles have been published on the topic, but there is still great mysticism associated with the SCS. This chapter presents a case study of the SCS and is an effort to grasp the contours of the system: how it works, what it encompasses, and how it affects the right to privacy and the principle of non-discrimination. The chapter concludes with a discussion on how we can understand the human rights issues posed in the SCS. Firstly, however, I present a theoretical context of surveillance, social control and modernity in China.

4.1 Surveillance, social control and modernity in China

Bakken characterizes modernity in China as both a process and a political agenda combining memories of the past and dreams for the future.[157] The pragmatic relationship between tradition (as memories) and modernity (as dreams) forms the foundation of social control in China. Tradition is an anchor point in a modern society characterized by chaos, too many choices, consumerism and risk.[158] The view of a dualistic modernization was emphasized in chairman Hu's report at the National Congress in 1982, where he advocated the need for building both a material and spiritual civilization in order to reach a socialist and stable civilization.[159] The speech sought to bring control into the chaotic modernization process, and

[157] Bakken, *The Exemplary Society*.

[158] Ibid., 17.

[159] Hu Yaobang as quoted in ibid., 54.

was "a battle-cry for taming the monster of modernization".[160] Hence, tradition represents a necessary break on fast-moving modernization processes, and it can mitigate modernization's so-called "spiritual slide" through social control, in a quest for stability within modernity.[161] Exemplary behavior based on the normative and binding character of tradition can thus be the antidote to the dangers of modernity. The emphasis on exemplary behavior and morality shows a belief in social engineering and governance. Modernization in this context is not only about technological and economic development, but also just as much about human development, with behavior as an integral part of the control system. Technological change does not simply relate to hardware and machines, but also to disciplinary technology related to spiritual improvement.[162] Science in this context is an objective instrument, one that may build a bridge over the tensions that arise between past and future. Yet, as Bakken points out, Chinese scientism is highly moralistic, and exemplarity is equal to objectively correct behavior.[163] This belief in objectivity is interesting in relation to the SCS, where both morality and data are believed to be objective truths against which individuals can be measured.

A central feature of social governance in China is the use of modelling as a way of promulgating the exemplary norms and virtue.[164] There is a fundamental belief that humans are capable of learning and changing.[165] This is not only related to individuals, but also groups such as companies or households. For example, in 1990, a county in Suzhou started the "drive to become ten-star civilized spiritual households".[166] Households were evaluated and accordingly awarded stars that were hung by their gates. This campaign reportedly had several positive effects in the county. It specifically emphasized education, and as a result, fewer parents took their daughters out of school. Crime rates allegedly dropped, the number of gang members decreased, and wealthy persons gave more money to charity.[167] Although one might question the validity of the data behind these claims, it can demonstrate the openness of Chinese people towards these types of social rewards systems, where exemplary behavior leads to social status, and where there is belief that humans are prone to change, and exemplarity is a

[160] Ibid., 55.
[161] Ibid., 18.
[162] Ibid., 51-52.
[163] Ibid., 52.
[164] Ibid., 169.
[165] Ibid., 173.
[166] Ibid., 175-76.
[167] Ibid., 176.

virtue that can be taught. It also shows the importance of publically parading virtue and morality as a way of inspiring others to live moral and virtuous lives.[168] Models emerge from below as a personification of morally superior, yet (barely) achievable values, and central modelling characteristics are family harmony and filial piety. A classic example from the Mao era is the young soldier Lei Feng, who is portrayed as a model citizen and a communist legend. Political campaigns urged people to "Live like Feng"[169] and do good deeds. The story is contested, and it is questioned whether the story of Lei Feng has resonance with Chinese people anymore, and whether he really does play an important role in maintaining social control, or whether there are other variables with a stronger explanatory power.[170] Nevertheless, the story illustrates the importance of modelling in Chinese politics, which is also an integral part of the SCS, where "redlists" with exemplary individuals and entities are publicly displayed.[171] In fact, Lei Feng is explicitly mentioned in the Planning Outline for the SCS, where the government calls for activities on trustworthiness, such as a "Lei Feng activity day".[172]

China is often criticized for its lack of liberal democratic structures, institutions, and civil and political rights, as well as its hesitance to sign and ratify international human rights treaties. Further, typical values in Chinese society and politics include communitarian values, where common rights and duties prevail when balanced with individual rights. In Confucianism, filial piety is considered the highest moral virtue and the family unit functions as an organizing principle for the state. This means that the government or state leader represents the family father who must make decisions for the greater good of the family.[173] Stability is also considered a crucial element in China's development and progress.[174] These different notions are often described as *human rights with Chinese characteristics*, indicating that how we understand human rights is not universal, but rather depends on historical and social circumstances. Song argues that we must consider Chinese political culture when we assess the SCS, and that "there are different cultural expectations of the government in China than in other countries".[175] She reiterates the idea that social governance has a long tradition in China. As

---

[168] Ibid., 175.

[169] "活雷锋", now used to describe a selfless person: *China.org.cn*, "Reviving the Lei Feng Spirit."

[170] *The Exemplary Society*, 185.

[171] Creemers, "Cyber China."

[172] State Council, "Planning Outline."

[173] Chan, "Human Rights and Democracy with Chinese Characteristics?," 649.

[174] Ibid., 646.

[175] Song, "The West May Be Wrong," 34.

the economy has developed and living standards have improved, fraud and crimes have proliferated and enforcing court decisions is difficult. Thus, the SCS's aim to strengthen trust and mitigate the challenges of technological development and modernity is welcomed by many. Song calls for an open-minded discussion where we consider the political and cultural context "[r]ather than instantly dismissing China's unconventional governance innovations".[176]

The term "credit" denotes several different ideas in Chinese, including integrity, credit, reputation or credence.[177] Historically credit has been used to assess morality and ethics. Thus, credit as a tool for social governance is not new in China; neither is gathering information on citizens' merits and behavior.[178] The personal file, *dang'an*, gathers minutia on both personal and professional information. It was introduced under Mao's regime, and contains information about employees' political opinion, family background, job history, education, mistakes, achievements, etc.[179] The file's content is unavailable and unchangeable to individuals. According to Yang, the *dang'an* was part of the government's methods of producing "the human subject as a passive object of administrative intervention", but it has now been revised to benefit the market economy.[180] Like the SCS, the *dang'an* is part of a bureaucratic power structure that is both overt and clandestine, and that intimately governs people's behavior and opportunities.[181]

Based on the depictions above, we can conclude that China has a long tradition of institutionalized offline surveillance. However, the SCS is far from the first technological system of surveillance in China. Since the introduction of the internet, the Chinese "netizen" population has grown substantially, yet the government still exercises effective control of the online sphere with meticulous censorship through programs such as the popularly named "Great Firewall of China".[182] Guo and Feng even find that young people in China support Internet censorship. Several variables might explain support for surveillance and censorship in China, and accurately measuring support for government programs in authoritarian regimes with limited freedom of speech will always be difficult. Nevertheless, the depiction of the SCS as something new and unique even in the Chinese context seems misplaced. Regardless

[176] Ibid., 35.
[177] Liang et al., "Constructing a Data-Driven Society," 424.
[178] Ibid.
[179] Yang, "The Politics of the Dang'an," 508.
[180] Ibid., 509.
[181] Ibid.
[182] Guo, Feng, "Understanding Support for Internet Censorship in China."

of whether we "instantly dismiss" the SCS, we can conclude that it has not arisen from a vacuum, and several researchers demonstrate high levels of approval for the system.[183]

4.2 The social credit system (SCS)

The SCS aims to rank Chinese citizens, companies, organizations and government entities by their trustworthiness. Trustworthiness is awarded as credit points based on compliance with legal, moral, and professional norms and standards. The accumulated credit score can affect one's possibilities in life, as those with a high score will be offered certain advantages while those with a lower score are sanctioned in different ways. Persons with a low score can receive education and can take steps to heighten their social score. The goal is to encourage trustworthiness and sanction untrustworthiness,[184] which will contribute to streamlining the market, and foster social governance towards the ultimate goal of building a harmonious, socialist society.[185] In other words, under the SCS exemplary behavior pays off.

As shown in the previous section, the idea of social governance and enforcing rules based on moral and exemplary conduct has long been the norm for governance in China.[186] Morality and law are in most liberal democracies seen as two separate spheres. In China, however, the relationship between morality and law resembles the relationship between law and norms in liberal democracies. Based on a belief in people's malleability, this system of punishment and education will lead to a material and spiritual development and social stability.[187] According to the government, the SCS is necessary in order to address problems in financial and commercial sectors, such as fraud, corruption, and debt.[188] Hoffman describes the system as a "feedback loop", which shapes, manages and responds to the behavior of citizens.[189] It is not only a top-down system of social control, but also encourages people to self-monitor and adjust their behavior accordingly. Further, the government encourages peer-to-peer surveillance by awarding points to people who report on others' misbehavior.[190] The

[183] Kostka, "SCS and Public Opinion".
[184] Chen, Cheung, "The Transparent Self," 357.
[185] State Council, "Planning Outline."
[186] Bakken, *The Exemplary Society*, 220.
[187] Ibid., 232.
[188] State Council, "Planning Outline."
[189] Hoffman, "Programming China," 1.
[190] State Council, "Planning Outline."

SCS also enables joint disciplinary action. This means that if a citizen does not comply within one legal area, she may receive sanctions within another legal area. For example, refraining from paying your taxes could mean that you are barred from traveling by airplane. Several agencies have also published "blacklists" of untrustworthy persons, and private actors are introducing their own social credit schemes. Liang et al therefore construe the SCS as a "*state surveillance infrastructure*", as it encompasses all social, economic and political domains, and the boundaries between the private sectors and the state are increasingly blurred.[191]

The SCS is a comprehensive big data strategy, which includes collecting personal data from all citizens, as well as data on public and private entities. It is a "penetrative system of personal data processing", in line with the Chinese government's ambitious plans for harnessing the benefits of big data technology.[192] Data is gathered through extensive monitoring of activities such as internet traffic, transactions, mobile phones, and CCTV cameras with facial recognition technology. Thus, the SCS uses both online and offline sources, and both public and private applications of big data, in order to create an enormous catalogue of information about Chinese citizens and entities. With China's "netizen" population and internet penetration rate growing significantly, personal data is constantly becoming more available to the government.[193] The SCS is not a single system (*yet*, as noted by Kostka), but an interweb of different commercial and governmental systems of ratings, sanctions and rewards.[194] The government's outline of the system calls for the establishment of several credit systems within four main areas: the governmental, commercial, social, and the judicial areas.[195] Most of the measures that are part of the SCS are directed at tackling corruption, improving efficiency in administrations and courts, and punishing unethical behavior of especially trust-based professions.[196] However, we can already see individual social effects of the SCS. By August 2016, five million attempts to purchase an airline ticket had been blocked, due to customer defiance of court orders.[197] Judgment defaulters are also frequently barred from travelling with high-speed trains, and information about them can be published on local, provincial or national

[191] Liang et al., "Constructing a Data-Driven Society," 426, 31.
[192] Chen, Cheung, "The Transparent Self," 356.
[193] Ibid., 360.
[194] Kostka, "SCS and Public Opinion". 1.
[195] Song, "The West May Be Wrong."
[196] Ibid., 34.
[197] *The Economist*, "China invents the digital totalitarian state."

credit websites. The SCS can also determine where one can be employed, as well as which schools one's children can be enrolled in.[198]

As mentioned, private actors also engage in credit scoring schemes. Alibaba launched its own credit scoring system in 2015, the *Sesame Credit*, which rates users based not only on what they purchase, but also on their friends' spending habits. Sesame scores can decide people's insurance premium, how they are screened at airport security, or where they are placed on an online dating service.[199] As such, the Sesame score can have an impact on the daily lives of its users. Although the system offers convenience to many citizens, "benefits and convenience to some mean sanctions and exclusion for others".[200] The Sesame score is voluntary; hence, its (extensive) reach is limited to those who opt in as customers. The mandatory nature of the SCS, on the other hand, means that the scope and reach can be unlimited, and the possibilities for sanctioning methods are manifold.[201] Private actors are also collaborating with the government in the establishment of the centralized credit infrastructures. Their data is used to improve the central credit system, and the companies receive data from the government databases in return.[202] For instance, the multi-purpose social media app WeChat shares data from their one billion users with the Chinese government based on a range of activities such as social interactions and online shopping. Citizens in local credit systems can reportedly check their personal score via WeChat.[203] Local authorities have also introduced social credit initiatives and pilot programs.[204] Shanghai's city government even introduced filial piety as part of the credit scoring system, whereby citizens could gain or lose points depending on how often they visited their parents.[205]

If we analyze the SCS as a surveillance system, or *surveillance infrastructure*, we can conclude that it is a multi-stakeholder system involving practically all actors in society, ranging from government agencies and officials, to corporations of different sizes, to groups and individuals. The surveillance is both top-down, i.e. from government or corporation to the individual, or from government to corporation, and horizontal, i.e. from peer to peer. Accord-

---

[198] Chen, Cheung, "The Transparent Self," 362.

[199] Ibid., 361.

[200] Ibid.

[201] Liang et al., "Constructing a Data-Driven Society," 427.

[202] Ibid., 431.

[203] *The Economist*, "China's "social credit" scheme."

[204] E.g. Suining County's credit system, where "trustworthy" citizens were rewarded with work promotions, speedy processing of public housing application, etc. See Chen, Cheung, "The Transparent Self."

[205] *Wall Street Journal*, "China's New Tool for Social Control."

ing to the government's Planning Outline, it will also be possible for citizens to access information about government agencies and companies, although the details remain unclear. Data generation is decoupled from data analysis. Thus, third parties are also involved in the surveillance practices, and data subjects do not necessarily know how their data is used.

Further, the modes of surveillance are also scattered and wide-ranging, including both online and offline techniques of surveillance, big- and "small" data, collected both in the private and public sphere, and with an extensive reach. The capacity for surveillance is dramatically advancing as the government utilizes new technologies.[206] These technologies also allow for a more subtle and covert surveillance in comparison with traditional tools, as political goals are embedded within algorithms. Thus, data ownership determines power distribution, and data sharing leads to an obfuscation of transparency and accountability.[207] This obfuscation is further snowballed by machine learning algorithms that process behavioral data and produce credit scores. The system is regulated by national and local legislation, but there is still a significant lack of adequate legal frameworks to protect privacy and personal data. Further, it remains to be seen whether *all* government entities will be subject to the system, or if certain segments of the top leadership in the Communist party will be exempt from behavioral scrutiny. As a top-down surveillance system, the SCS resembles Bentham's panopticon. On the other hand, the system is more fragmented and multi-faceted than what we might expect from the classic prison panopticon, and it would perhaps make more sense to talk about it as systems rather than a single, unified system.[208]

While several other jurisdictions use different forms of credit scorings, the SCS is unique in its scope, particularly through reaching far beyond financial credit scoring and criminal records, and the lack of regulations limiting the intrusive power of the state. From a Western perspective, the SCS thus seems like an obvious obstacle for true enjoyment of human rights in China. The enhancement of surveillance practices enabled by new technologies is likely to augment the existing human rights challenges that the Chinese system of social government poses. China has international human rights obligations, and the country is a signatory to the ICESCR and the ICCPR, but it has yet to ratify the latter.[209] Regardless of whether we adopt a universal or relativist approach to human rights, it is imperative to assess

[206] Liang et al., "Constructing a Data-Driven Society," 429.
[207] Ibid., 420.
[208] Kostka, "SCS and Public Opinion".
[209] Human rights in China, "UN Treaty Bodies and China".

actual and potential human rights issues posed by the SCS. The following two sections will examine challenges to the rights to privacy and non-discrimination posed by the SCS.

4.3 The SCS and the right to privacy

The right to privacy as enshrined in the ICCPR is obviously challenged by the SCS. Through invasive surveillance activities, the SCS will retrieve information from practically all segments of people's social and private lives. In the Universal Periodic Report carried out on China in 2018, civil society actors noted with concern that "[d]raconian cyber policies had been codified into law", and that Chinese cyber security laws have substantially increased internet surveillance and restricted the freedom of expression on the internet.[210] As discussed in chapter 2, any surveillance data must be used for the specific legitimate and legal purposes it was intended for. Under the SCS, different sectors and organizations will share information between them.[211] This means that the data will be analyzed in other contexts than for what it was collected. Thus, data generation is decoupled from data analysis, and violations to the right to privacy in one surveillance phase can be scaled in another. Further, the Human Rights Watch criticized the authorities' collection of biometrics in Xinjiang, arguing that the practice is not compatible with the right to privacy under international human rights law.[212] The government's Planning Outline does include references to the rights of individuals in general, and the right to privacy in particular. It remains unclear, however, how the privacy of individuals will be maintained in a system founded on collecting and sharing intimate personal data.

The right to privacy under the SCS is severely limited, as intimate details about people's private and social lives are *datafied* with a complete lack of consent. This data is collected and scrutinized for social control purposes, and the government can use both data and metadata for predictions and policymaking. The right to be forgotten introduced in the GDPR, as well as the question of re-identification, are absent in this context, as storing troves of personal data is at the very core of the system. As such, China is winning the digital AI race, as IT developers have unlimited access to data, at least in comparison with developers in European countries with strict regulations for personal data. AI expert Morten Goodwin notes that more data is needed to develop transparent and advanced AI. He claims that developers in

[210] UNGA, "Stakeholders' submissions on China," 34-35.

[211] State Council, "Planning Outline."

[212] UNGA, "Stakeholders' submissions on China," 42.

Norway do not have sufficient data to be able to create *descriptive* algorithms, i.e. algorithms that explain the choices they have made.[213] Chinese developers are therefore in a unique position, receiving ample government funding to develop algorithms and AI freely and rapidly, without having to anonymize, fuzzy or restrict their use of data.[214] Privacy within the SCS is therefore also highly contingent on data security. China allegedly has "a poor record of data security" and personal information is easily accessible, which makes the SCS vulnerable to hacking and illegal access.[215] As the SCS collects personal data, including biometric data as has been reported, and there is no incentive or system for anonymization of data, criminals hacking the SCS could constitute a failure of the state to both protect and fulfil its obligations under the right to privacy.

The SCS challenges the right to privacy both in terms of data collection through extensive surveillance, and in terms of data sharing between different entities, including between private and public actors. Digital traces are not only used for targeted marketing or improving online services, but are also used to train AI and inform the government on habits, activities and actions. Public surveillance cameras with facial recognition technology grant the government close to full and constant access to all public spaces, and digital surveillance through large tech companies provide the government with information on citizens' private and social lives. Peer-to-peer surveillance offers the government offline access to otherwise unavailable social spheres. The use of machine learning algorithms to process the data, in addition to widespread data sharing practices, leads individuals to lose ownership of their personal information.[216] All this can substantially affect the right to privacy in addition to several other human rights. The next section assesses the relationship between the SCS and the principle of non-discrimination.

4.4 The SCS and non-discrimination

The SCS can lead to discriminatory practices in several ways. Firstly, despite the plans of unifying the systems into a national credit system, it will still be up to local governments and administrations to determine the criteria against which individuals are judged. With the

[213] *NRK*, "Kina vinner det digitale kappløpet."
[214] Qiang, "The Road to Digital Unfreedom."
[215] *The Economist*, "China's "social credit" scheme."
[216] Chen, Cheung, "The Transparent Self."

lack of a uniform standard, citizens are at the mercy of their local government. Peasants in the countryside might then be under a different credit scheme than people in urban areas.[217] Further, as data moves between sectors and agencies, flaws in data in one database can be replicated throughout all the databases that the data passes by. As such, any data bias that is not appropriately mitigated will continue with the data flow, and perhaps even grow or change in a different context.[218]

As argued in chapter 3, it is close to impossible to obtain purely objective data. Thus, labelling data as "objective" or "raw" can be harmful because it clearly overlooks the potential bias in data. It is equally difficult to create an objective machine-learning algorithm by which to process the data and rank citizens, we well as to ascertain how the algorithm will react to new data. Although bias can be mitigated, this requires an acknowledgement of the existence of bias. This does not seem to be the case in China. According to the Planning Outline, there are plans to "[g]uarantee the objectivity, truthfulness, accuracy and timely updating of credit information", which could indicate an effort to mitigate biased data.[219] However, according to Bakken, moral behavior equates to objectively good behavior in Chinese culture, hence there is a belief in the possibility of objectively rating citizens' trustworthiness.[220] This negligence in mitigating data bias in big data analysis might pave the way for discriminatory activities such as predictive policing. On the micro level, "suspicious" correlations based on big data predictions can be used against individuals, for example by again hindering them from flying or enrolling their children in a private school. As mentioned in chapter 3.3, however, risk predictions do not work on the individual level, and such predictive policing would likely constitute a violation of the right to equality before the law. On the macro level, the SCS can inform the government on trends, public opinion, and possible challenges in society, which can assist the government in predictive social control and policy-making.[221]

Another issue raised regards discrimination by association, as there have been reports that children are discriminated based on their parents' low score.[222] Further, the disproportionality of punishment might imply that a person who has not paid a parking ticket will not be permitted to fly home to see his family for the holidays, quite a harsh punishment for a

---

[217] *AsiaGlobal Online*, "Trust in Ratings."

[218] Ibid.

[219] State Council, "Planning Outline."

[220] Bakken, *The Exemplary Society*, 259.

[221] Liang et al., "Constructing a Data-Driven Society."

[222] Chen, Cheung, "The Transparent Self," 362.

petty "crime". In this regard, the system also needs to be developed carefully to not have a sort of domino effect, where neglecting one's parents leads the person to be placed on the no-fly list, which again hinders the possibility of visiting her parents. On the other hand, however, according to regulations, blacklists will only contain persons how have not met their legal obligations, i.e. by not showing up in court or by refusing to pay a fine, and not people who have "only" accumulated a bad credit score based on "misbehavior" such as filial impiety.[223]

Who will be the victims of the SCS? According to some, the losers will be minorities, both sexual, religious, and ethnic minorities.[224] It has been reported that there are already more than a million minorities in prison camps in the Xinjiang province, most or all of them belonging to the Muslim Uighur minority.[225] Minorities in China already face systematic discrimination, but the SCS could augment discriminatory practices, and affect social mobility within these groups.[226] This raises the important question of *what* the government regards as moral behavior. For instance, does being openly homosexual constitute moral behavior? After a revision of Chinese criminal code in 1997, homosexuality is no longer considered "hooliganism".[227] There have been reports that conditions for LGBT+ persons are improving, and the concept of *tongzhi* (homosexuality) is increasingly becoming known and visible in society. Openly gay couples are perhaps not common but certainly present in China, the city of Chengdu in Sichuan has been coined the "San Francisco of China"[228] and LGBT+ dating apps boast millions of users. Some academics argue that China's growing gender imbalance may be good news for homosexuals.[229] After years of extensive female discrimination at birth, millions of men are in "marriage age" without a potential partner, which may increase acceptance for men who choose to live in a same-sex relationship. On the other hand, this may be bad news for lesbian women, who may face even more pressure on leading a traditional heterosexual family life for the sake of reproduction. Furthermore, there are stories of LGBT+ dating apps being shut down, Pride celebrations and demonstrations being banned, and activists being persecuted. Clearly, the SCS can move these challenges in different directions, and an assessment of the SCS must be sensitive to the different effects that the system can have on

---

[223] Daum, "Who did China ban from flying?"., *The Economist*, "China's "social credit" scheme."

[224] Future Thinkers Podcast, *Anti-Authoritarian Technologies*.

[225] *BuzzFeed*, "China is Vacuuming up DNA Samples from Xinjiang's Muslims."

[226] Ibid.

[227] *Foreign Policy*, "It's Still (Just About) OK to Be Gay in China."

[228] I.e. the "gay capital of China".

[229] Zheng et al., "Sociosexuality in Mainland China."

vulnerable groups. Reports already show that the Uighur minority in Xinjiang province live in a surveillance state, with egregious narratives of widespread discrimination based on ethnicity and religion, as well as Uighur's being subject to biometric surveillance and inhumane treatment in detention camps.[230] Again, systematic discrimination of ethnic minorities is not a new concept in China, but technologies that allow for collection of biometric data, facial recognition and other surveillance tools may have substantially increased the scale and reach of these human rights violations.

In summary, the SCS both highlights existing challenges to the rights to privacy and non-discrimination, and it challenges these rights in new and more invasive ways, assisted by the government's innovative use of technology and lack of personal data regulation limiting the use of data. The next section will discuss how the SCS might serve as an illustration of how new technologies are transforming the human rights challenges posed by surveillance, or whether the system is uniquely Chinese statistical outlier as a case.

4.5 Surveillance, technology, human rights and the social credit system

Bakken's depiction of Chinese society and social control highlights the fact that the ideas behind the SCS are nothing new. Evaluation and social credit scores have long been integral parts of the educational system, as well as at work and other social spaces.[231] Modelling has been a central part of systems for social control, as it is in the SCS as well. The *dang'an* file as an analogue *data double* has kept intimate details about citizens over several decades. However, these practices of social control are augmented by the Chinese government's innovative use of technologies such as big data and AI. The SCS resembles a combination of both tradition and modernity, as it recalls virtues of the past, while utilizing technologies and aims to strengthen economic and spiritual development for the future. Mechanisms of tradition will lead to a more trustworthy society and tame the wild beast of modernity, so to speak. The government will no longer depend on violence for repression, as they can count on citizens to control each other and themselves. This "innovative social governance", as coined by president Xi Jinping, will "improve the capability to predict and prevent security risks."[232]

---

[230] *BuzzFeed*, "China is Vacuuming up DNA Samples from Xinjiang's Muslims."

[231] Bakken, *The Exemplary Society*.

[232] *China Daily*, "Security innovation seen as crucial."

Depending on the definition of "security risks", we may see a rise in predictive policing as a result of the implementation of the SCS.

These ambitions for social governance in the SCS suggest that we are indeed moving from a disciplinary society to a society of control. Surveillance is high-tech and less physical, and the government can use their power to control access and tie together the loose knots of a fragmented society.[233] The SCS also uses *dataveillance* in order to govern people's behavior.[234] With its ever-increasing population of netizens, technology is now at the core of social and economic control in China. However, these new technologies can also be used for productivity across sectors, for improving public services such as health and education, and for policymaking. Thus, there is a tension between information technology's potential for democratization and emancipation, and the Chinese government's ability to control the information flows.[235]

Throughout my period of research, I have also entertained the idea that the system might actually work. Crime rates could drop; instances of domestic violence could decrease; people could start recycling their waste; and companies could take social responsibility. Moral governance might be the only viable solution to the perceived moral decay caused by the monster of modernity. The SCS can ensure that our accumulated social score based on good behavior decides our possibilities in life, rather than arbitrary financial metrics such as the balance in our bank account. Furthermore, we trust large corporations with vast amounts of our personal data, and it is worth asking the question whether the government is any different. Perhaps the government is different because it has a monopoly of legitimate violence and can limit our access to freedoms and services on a broader scale.[236] This argument, however, depends on the premise that government is fair, transparent and accountable, and that corporations will never become big enough to hold that sort of power. In the case of the Sesame score, this has already proven to be false. A private company has clearly managed to restrict freedoms for ordinary citizens. This is also the case in liberal democracies, such as when insurance companies in the United States start to use data from social media in order to determine insurance premiums. This clearly resembles a social credit-scoring scheme.[237] A difference between corporate credit schemes and the SCS is the possibility to opt out. Having a

[233] Deleuze, "Postscript on the societies of control," 5.

[234] Esposti, "When big data meets dataveillance."

[235] Creemers, "Cyber China," 86.

[236] Focarelli, *International Law as Social Construct*, 10.

[237] *The Wall Street Journal*, "Can a Facebook Post Make Your Insurance Cost More?."

Sesame score or subscribing to a specific insurance policy is voluntary. However, if we opt out from whichever platform that wants to collect our data, we might not be able to fully participate in a modern society. Further, users share much of their information unknowingly, and lose control over their personal data. Alibaba, for instance, gets most of its data from other databases than their own, and these are mainly owned by the government.[238] As it turns out, this is not a uniquely Chinese practice. In May 2019, it was reported that the American airline company JetBlue received biometric data from the US government in order to have passengers board by facial recognition instead of boarding passes.[239]

Despite potential benefits of the SCS, it clearly poses challenges to both the right to privacy and non-discrimination, in addition to several other human rights. Although the Planning Outline indicates that citizens can file complaints and hold their local government accountable, this is not necessarily the case in practice.[240] Liang et al. argue that the sphere of accountability has diminished as the ability for the Chinese government and commercial actors to monitor the populace has increased.[241] This is not only the case in China. The post-9/11 increase in surveillance practices and the so-called chilling effect of surveillance already affect our behavior, according to scholars.[242] Further, the "nothing to hide" mentality indicates that many of us are not worried about invasive surveillance, as long as there is a perceived need for it in order to ensure the safety and security of citizens. We might not even notice a shift towards the Chinese model. China argues that the system is a solution to moral decay, to societal instability and a lack of trust. In other words, the government argues that a perceived threat can be minimized with a sanctions and rewards system through surveillance, much resembling the mode of reasoning from Western governments as well. Furthermore, Western democratic leaders are often reluctant to include morality as the basis for a political argument, but with the rapid development of AI, it is pressing to discuss ethical considerations in data and algorithms. The Chinese might even be superior in terms of their moral vocabulary.

Moreover, with the omnipresence of Chinese companies and interests, Hoffman expresses concern over the global consequences of the SCS, and urges democratic nations to strengthen their own data protection regulations and proactively counter the development and

---

[238] Liang et al., "Constructing a Data-Driven Society," 431.

[239] *NRK*, "Facial Recognition: - You Should Be Worried."

[240] State Council, "Planning Outline."

[241] Liang et al., "Constructing a Data-Driven Society," 434.

[242] Solove, ""Nothing to Hide"."

expansion of social credit in China.[243] The Planning Outline also includes plans to cooperate with credit rating bodies in other countries, and the government has proposed a transnational "Belt and Road Initiative" credit system to secure economic relations and international trade.[244] Jack Ma, the founder of Alibaba, urged the Canadian government to use the Sesame score for granting expedited visas for Chinese tourists. Henceforth, both the Chinese government and corporations have global ambitions to expand social credit schemes.[245] We might even see Western regimes become interested in the technology and know-how of the SCS if it is successful in altering citizen behavior and increasing productivity.[246]

We can conclude that the SCS may offer conveniences and solutions to certain societal issues, but this will happen at the expense of several recognized human rights. At the very least, the system resembles social sorting and what Lyon argues is a modern way of forming docile populations.[247] The SCS may not dramatically change the underlying causes of human rights challenges present in China today, but the innovative use of technology, the streamlining of bureaucracy and cross-sectoral communication, and the extensive data sharing practices within a system that lacks an adequate protection of privacy are likely to augment these challenges. The system is founded on a belief that individuals can be measured against an objective, moral norm, resembling Foucault's panoptic theory.[248] Further, big data technologies and AI contribute to diminishing the sphere of accountability, and enlarging the power asymmetry and distance between the citizen and the government, and the citizen and corporations.

Chapter 3 highlighted that AI and big data significantly challenge a number of human rights through altering and scaling existing issues. They enable invasive surveillance practices, and they can help obfuscate human rights abuses. Data subjects, or citizens, lose ownership over their own personal information, and information asymmetry leads to a lack of awareness – citizens do not necessarily know that their rights are being violated. Further, if we overestimate the objectivity of input data, any efforts in mitigating potential bias will be insufficient. Thus, these new technologies risk posing a challenge to both the right to privacy and the principle of non-discrimination, as well as other human rights that are not touched upon in this thesis. The case of the SCS in China carries several of the same challenges as

[243] Hoffman, "Social credit," 3.

[244] State Council, "Planning Outline."

[245] Liang et al., "Constructing a Data-Driven Society," 435.

[246] Nemitz, "Constitutional Democracy and Technology," 2.

[247] Lyon, *Surveillance studies*, 4.

[248] Galič et al., "Bentham, Deleuze and Beyond," 17.

broader developments in liberal democracies as well as in authoritarian regimes like China. The SCS might be unique in what resembles a gamification of social life, but it is not necessarily unique in terms of moving towards a society with widespread surveillance, less privacy and potentially more discrimination. As such, challenges to the right to privacy posed by the SCS are probably less distinctive than the way in which the SCS affects the principle of non-discrimination. A key issue that at least on paper separates China from liberal democracies, however, is the lack of separation of technology and state, or corporations and state, as well as a lack of checks and balances to scrutinize and limit the power of the government.[249]

[249] Nemitz, "Constitutional Democracy and Technology."

5 Conclusion

This thesis has addressed a few pressing issues in the nexus of surveillance, technological development and human rights. In order to answer the first research question on how surveillance challenges the rights to privacy and non-discrimination, chapter 2 presented different surveillance theories. These teach us how to recognize surveillance practices, and how to study them in light of the actors involved, the different modes of surveillance, and the regulations against which they are measured. Surveillance challenges the right to privacy and the principle of non-discrimination in different ways. The core practice of surveillance is gathering information, and as such, it clearly challenges the right to privacy, not only in the data collection phase, but also in the ways in which data is analyzed and used for decision-making. Further, surveillance may harm the principle of non-discrimination in terms of the selection criteria for subjects and data, as well as in consecutive phases of surveillance.

Chapter 3 showed that human rights challenges can be significantly augmented by the introduction of technologies such as AI and big data, although the underlying causes of human rights abuse probably are not as affected by technology. Further, the introduction of new technologies can bring about *new* human rights issues. Henceforth, lawmakers must have a sound understanding of technical solutions, and similarly, IT developers should include a form of human rights due diligence when building new technologies.[250] The issue is more nuanced than a pro-or-con dichotomy might show, and despite the potential dangers of new technologies, it is difficult to imagine a development where societies become *less* dependent on technology. The SCS, as presented in chapter 4, perhaps represents a dystopic prophesy of what happens when technologies and tech companies are allowed to develop freely without the restriction of privacy laws, or without a separation of state and technology. These issues suggest that we need to incorporate human rights when we build new technologies, and there needs to be checks and balances in place to limit both governments'- and states' collection of our personal data.

The media often sensationalizes the SCS. It might very well be an extreme case, yet it encompasses several human rights issues that are present in democratic and authoritarian regimes alike. Technological development has brought new opportunities for human rights in China as it has elsewhere, especially social and economic rights, yet they also pose challenges to rights such as the rights to privacy and non-discrimination. The SCS both augments exist-

[250] McCorquodale et al., "Human Rights Due Diligence."

ing human rights challenges, much like the Saudi government's app for social control, yet it likely also introduces new human rights issues in China. At the time of writing, however, it is difficult to say how these challenges will play out in practice. The SCS has been introduced in a context where social control and surveillance are not foreign ideas. This is quite self-evident – policy arguably arises within a social or cultural context, but new technologies enable a far wider reach for these practices. China is positioning itself as a leader in AI, and with a lack of regulations protecting privacy and personal data, they might very well be winning the "digital race". Thus, predicting the potentially innovative future of China's "digital dictatorship"[251] is not something that can be done within the scope of a Master's thesis.

New technology both scales existing human rights challenges, and has the potential to transform the nature of human rights issues. Further, technological development can challenge existing privacy laws, and according to some, render them outdated. Others claim that many existing privacy regulations are technology-neutral, such as the GDPR. Thus, further research is needed on the area of consent, privacy law and technology, perhaps especially within the law-in-context methodological field. In many ways, internet presence and participation in various social media are part of being a citizen in a modern society. New research could focus on how human rights regulations and legislation can adapt to big data and technological development within consent-based services like online shopping and social media.

New technologies can also bring opportunities for the enjoyment of human rights. Both organizations and companies are experimenting with using new technologies to fulfil and promote human rights, or help human rights defenders.[252] Future research for human rights scholars interested in technological development should investigate how we can govern technology to be accountable, transparent and fair. Assessing how technology can develop without harming human rights is imperative as we continue to move towards a smart, technological society.

[251] *The Wall Street Journal*, "Stranger Than Science Fiction."

[252] E.g. Whistler., *Flash Drives for Freedom*, or Amnesty International's Virtual reality project, placing participants in war-torn Aleppo to raise awareness and donations.

6 Bibliography

Legal sources

EU General Data Protection Regulation (GDPR). 2016. Regulation (EU) 2016/679.

R v. Immigration Officer at Prague Airport and another (Respondents), ex parte European Roma Rights Centre and others (Appellants), UKHL 55 (2004).

Robert W. Gauthier v. Canada, (1999).

United Nations General Assembly (UNGA). *Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)*, 1979. Vol. 1249. United Nations Treaty Series,

United Nations General Assembly (UNGA). *International Covenant on Civil and Political Rights (ICCPR)*, 1966. Vol. 999. United Nations Treaty Series,

United Nations General Assembly (UNGA). *International Covenant on Economic, Social and Cultural Rights (ICESCR)*, 1966. Vol. 993. United Nations Treaty Series,

United Nations General Assembly (UNGA). *Universal Declaration of Human Rights (UDHR)*, 1948. Resolution 217 A (III).

Vice-President Ammoun's separate opinion to the International Court of Justice Namibia Advisory Opinion from 1971: "Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276, (1971).

UN and government documents

Human Rights Council (HRC). *Report of the Special Rapporteur on the right to privacy*, 2019. A/HRC/40/63.

McGregor, Lorna, Fussey, Pete, Murray, Daragh, and Ng, Vivian. "Submission to OHCHR. The Right to Privacy in the Digital Age." Essex University's Human Rights Centre, 2018.

Office of the High Commissioner for Human Rights (OHCHR). "The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights." 2014.

Special Rapporteur on the Right to Privacy. "Submission to OHCHR. Mandate of the Special Rapporteur on the Right to Privacy."

State Council. "Notice of the State Council on the Planning Outline of the Construction of a Social Credit System (2014-2010)." 2014. 国务院关于印发社会信用体系建设规划纲要（2014—2020 年）的通知. http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

United Nations General Assembly (UNGA). "Resolution 68/167. The Right to Privacy in the Digital Age.": United Nations General Assembly, 2013.

United Nations General Assembly (UNGA). "Summary of Stakeholders' submissions on China. Report of the Office of the United Nations High Commissioner for Human Rights." 2018.

United Nations Human Rights Committee. "Concluding observations on the fourth periodic report of the United States of America." 2014.

United Nations Human Rights Committee. "General Comment No. 16, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17)." 1988.

United Nations Human Rights Committee. "General Comment No. 18, Non-Discrimination." 1989.

Journal articles

Albrechtslund, Anders. "Online social networking as participatory surveillance." *First Monday* 13, no. 3 (2008).

Bolter, J. David. "Artificial Intelligence." *Daedalus* 113, no. 3 (1984): 1-18.

Cath, Corinne. "Governing artificial intelligence: ethical, legal and technical opportunities and challenges." *Philosophical Transactions* 376, no. 2133 (2018): 1-8.

Chan, Phil C. W. "Human Rights and Democracy with Chinese Characteristics?". *Human Rights Law review* 13, no. 4 (2013): 645-89.

Chen, Yongxi, and Cheung, Anne S. Y. "The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System." *The Journal of Comparative Law* 12, no. 2 (2017): 356-78.

Creemers, Rogier. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China* 26, no. 103 (2017): 85-100.

Deleuze, Gilles. "Postscript on the societies of control." *October* 59 (1992): 3-7.

Esposti, Sara Degli. "When big data meets dataveillance: The hidden side of analytics." *Surveillance and Society* 12, no. 2 (2014): 209-25.

Floridi, Luciano. "Soft ethics, the governance of the digital and the General Data Protection Regulation." *Philosophical Transactions* 376, no. 2133 (2018).

Fulton, Janet M., and Kibby, Marjorie D. "Millennials and the normalization of surveillance on Facebook." *Journal of Media & Cultural Studies* 31, no. 2 (2016): 189-99.

Galič, Maša, Timan, Tjerk, and Koops, Bert-Jaap. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30, no. 1 (2017): 9-37.

Guo, Steve, and Feng, Guangchao. "Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action." *Journal of Chinese Political Science* 17, no. 1 (2012): 33-52.

Haggerty, Kevin, and Ericson, Richard. "The surveillant assemblage." *British Journal of Sociology* 51, no. 4 (2003): 605-22.

Hallinan, Blake, and Striphas, Ted. "Recommended for you: The Netflix Prize and the production of algorithmic culture." *New Media & Society* 18, no. 1 (2016): 117.

Harambam, Jaron, Helberger, Natali, and Hoboken, Joris van. "Democratizing algorithmic news recommenders: how to materialize voice in a technologically saturated media ecosystem." *Philosophical Transactions* 376, no. 2133 (2018).

Harris, Robert. "Policy Analysis and Policy Development." *Social Service Review* 47, no. 3 (1973): 360-72.

Hoffman, Samantha. "Programming China: The Communist Party's autonomic approach to managing state security." *Merics China Monitor* 44 (2017).

Kostka, Genia. "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval." (2018).
doi: http://dx.doi.org/10.2139/ssrn.3215138, https://ssrn.com/abstract=3215138.

Kranzberg, Melvin. "Technology and History: "Kransberg's Laws"." *Technology and Culture*, no. 3 (1986): 544.

Levy, Jack S. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25, no. 1 (2008): 1-18.

Liang, Fan, Das, Vishnupriya, Kostyuk, Nadiya, and Hussain, Muzammil M. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure." *Policy & Internet* 10, no. 4 (2018): 415-53.

Liu, Hin-Yan. "The power structure of artificial intelligence." *Law, Innovation and Technology* 10, no. 2 (2018): 197-229.

Lyon, David. "Surveillance, Security and Social Sorting: Emerging Research Priorities." *International Criminal Justice Review* 17, no. 3 (September 2007): 161-70.

Lyon, David. "Surveillance, Snowden, and big data: capacities, consequences, critique.". *Big data & Society* 1, no. 2 (2014): 1-13.

McCorquodale, Robert, Smit, Lise, Neely, Stuart, and Brooks, Robin. "Human Rights Due Diligence in Law and Practice: Good Practices and Challenges for Business Enterprises." *Business and Human Rights Journal* 2, no. 2 (2017): 195-224.

Nemitz, Paul. "Constitutional democracy and technology in the age of artificial intelligence." *Philosophical Transactions* 376, no. 2133 (2018).

Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no. 1 (January 2019): 53-67.

Risse, Mathias. "Human Rights and Artificial Intelligence: An Urgently Needed Agenda." *Human Rights Quarterly* 41, no. 1 (2019): 1-16.

Solove, Daniel J. ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy." *San Diego Law Review* 44 (2007): 745-72.

Song, Bing. "The West May Be Wrong About China's Social Credit System." *New Perspectives Quarterly* 36, no. 1 (2019): 33-35.

Stoycheff, Elizabeth. "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring." *Journalism & Mass Communication Quarterly* 93, no. 2 (2016): 296-311.

Yang, Jie. "The Politics of the Dang'an: Spectralization, Spatialization, and Neoliberal Governmentality in China." *Anthropological Quarterly* 84, no. 2 (2011): 507-33.

Zheng, Wei Jun, Zhou, Xu Dong, Wang, Xiao Lei, and Hesketh, Therese. "Sociosexuality in Mainland China." *Archives of Sexual Behavior* 43, no. 3 (2013): 621-29.

Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30 (2015): 75-89.

Books and book sections

Bakken, Børge. *The Exemplary Society. Human Improvement, Social Control, and the Dangers of Modernity in China.* New York: Oxford University Press, 2000.

Davidson, Cathy N., and Savonick, Danica. "Digital Humanities: The Role of Interdisciplinary Humanities in the Information Age." In *The Oxford Handbook of Interdisciplinarity*, edited by Robert Frodeman: Oxford Handbooks Online, 2017.

de Schutter, Olivier. *International Human Rights Law.* 2 ed. Cambridge: Cambridge University Press, 2014.

Focarelli, Carlo. *International Law as Social Construct: The Struggle for Global Justice.* Oxford, United Kingdom: Oxford University Press, 2012.

Foucault, Michel. *Discpline and punish: the birth of the prison.* London: Penguin, 1991.

Gerring, John. *Case Study Research. Principles and Practices.* 2 ed. United Kingdom: Cambridge University Press, 2017.

Jr., Oscar Gandy. "Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment." In *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard Victor Ericson, 363-84. Toronto: University of Toronto Press, 2003.

Lyon, David. *The Electronic Eye: The Rise of Surveillance Society.* United Kingdom: Polity Press, 1994.

Lyon, David. "The search for surveillance theories." In *Theorising surveillance: The panopticon and beyond*, edited by David Lyon, 3-20. Portland: Willan Publishing, 2006.

Lyon, David. *Surveillance studies: an overview.* Cambridge: Polity, 2007.

Lyon, David, and Zureik, Elia. *Computers, surveillance, and privacy.* University of Minnesota Press, 1996.

Matzner, Tobias. "Grasping the ethics and politics of algorithms." Chap. 3 In *The Politics of Big Data. Big Data, Big Brother?*, edited by Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green, 39-46. New York: Routledge, 2018.

Matzner, Tobias. "Surveillance as a critical paradigm for Big Data?". Chap. 5 In *The Politics of Big Data. Big Data, Big Brother?*, edited by Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green, 68-87. New York: Routledge, 2018.

Mayer-Schönberger, Viktor, and Cukier, Kenneth. *Big Data. A Revolution That Will Transform How We Live, Work, and Think.* Mariner Books, 2013.

Schneider, Ingrid. "Bringing the state back in: Big Data-based capitalism, disruption, and novel regulatory approaches in Europe." Chap. 8 In *The Politics of Big Data. Big Data, Big Brother?* , edited by Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green, 129-76. New York: Routledge, 2018.

Schwab, Klaus. *The Fourth Industrial Revolution.* Geneva, Switzerland: World Economic Forum, 2016.

Sætnan, Ann Rudinow. "The haystack fallacy, or why Big Data provides little security." Chap. 2 In *The Politics of Big Data. Big Data, Big Brother?*, edited by Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green, 21-39. New York: Routledge, 2018.

Sætnan, Ann Rudinow, Schneider, Ingrid, and Green, Nicola. "The Politics of Big Data. Principles, Policies, Practices." In *The Politics of Big Data. Big Data, Big Brother*, edited by Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green. New York: Routledge, 2018.

Westin, Alan F. *Privacy and Freedom.* New York: Atheneum, 1967.

Yin, Robert K. *Case Study Research. Design and Methods.* 5 ed. USA: Sage Publications, 2014.

Newspaper articles

Almås, Gry Blekastad. "Digitalt diktatur: Kina planlegger sosialt poengsystem." *NRK*, April 5 2019, https://www.nrk.no/urix/kinas-digitale-diktatur_-gar-du-pa-rodt-lys_-blir-du-uthengt-pa-storskjerm-1.14369439, accessed 06.04.2019.

Arsène, Séverine. "Trust in Ratings: China's Social Credit System." *AsiaGlobal Online*, May 17 2018, http://dev14-7.ysdhk.com/asiaglobalonline/p01/china-social-credit-system/, accessed 21.04.2019.

Byron, Ellen, and Scism, Leslie. "Can a Facebook Post Make Your Insurance Cost More?" *The Wall Street Journal*, March 18 2019, https://www.wsj.com/articles/can-a-facebook-post-make-your-insurance-cost-more-11552915222, accessed 22.04.2019.

Chin, Josh, and Wong, Gillian. "China's New Tool for Social Control: A Credit Rating for Everything." *Wall Street Journal*, November 28 2016, https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590, accessed 15.04.2019.

"China's "social credit" scheme involves cajolery and sanctions." *The Economist*, March 28 2019, https://www.economist.com/china/2019/03/28/chinas-social-credit-scheme-involves-cajolery-and-sanctions, accessed 17.04.2019.

"China invents the digital totalitarian state." *The Economist*, December 17 2016, https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state, accessed 15.04.2019.

Dastin, Jeffrey. "Amazon scraps secret AI recruiting tool that showed bias against women." *Reuters,* 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G, accessed 18.04.2019.

Goodwin, Morten. "Kina vinner det digitale kappløpet." *NRK*, 06.02.2019 2019, https://www.nrk.no/ytring/kina-vinner-det-digitale-kapplopet-1.14415911, accessed 17.04.2019.

Johansen, Per Anders. "På tide å få bedre kontroll over kvinnene, tenkte sjeikene. Så fant de den perfekte metoden for å overvåke kona og døtrene." *Aftenposten*, February 16 2019, https://www.aftenposten.no/norge/i/9m7Pkw/Pa-tide-a-fa-bedre-kontroll-over-kvinnene_-tenkte-sjeikene-Sa-fant-de-den-perfekte-metoden-for-a-overvake-kona-og-dotrene, accessed 20.02.2019.

Lapowsky, Issie. "How Cambridge Analytica Sparked the Great Privacy Awakening." *Wired,* 2019, https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/, accessed 01.04.2019.

Palmer, James. "It's Still (Just About) OK to Be Gay in China." *Foreign Policy*, April 17 2018, https://foreignpolicy.com/2018/04/17/its-still-just-about-ok-to-be-gay-in-china/, accessed 21.04.2019.

Rajagopalan, Megha. "China is Vacuuming up DNA Samples from Xinjiang's Muslims." *BuzzFeed,* 2017, https://www.buzzfeednews.com/article/meghara/china-is-quietly-collecting-dna-samples-from-millions-of, accessed 20.04.2019.

Solheim, Eirik. "Facial Recognition: - You Should Be Worried." (Ansiktsgjenkjenning – du burde være bekmret) *NRK*, May 7 2019, https://nrkbeta.no/2019/05/07/ansiktsgjenkjenning-du-burde-vaere-bekymret/, accessed 08.05.2019.

Vincent, Alice. "Black Mirror is coming true in China." *The Telegraph*, 2017, https://www.telegraph.co.uk/on-demand/2017/12/15/black-mirror-coming-true-china-rating-affects-home-transport/, accessed 20.01.2019.

Wen, Gong. "A Guide to Reviving the Lei Feng Spirit." *China.org.cn*, February 28 2012, http://www.china.org.cn/opinion/2012-02/28/content_24752379.htm, accessed 22.04.2019.

Yuan, Li. "Stranger Than Science Fiction: The Future for Digital Dictatorships " *The Wall Street Journal*, March 1 2018, https://www.wsj.com/articles/stranger-than-science-fiction-the-future-for-digital-dictatorships-1519900866, accessed 20.03.2019.

Zhang, Yan. "Security innovation seen as crucial." *China Daily*, 20 September 2017, http://www.chinadaily.com.cn/china/2017-09/20/content_32225951.htm, accessed 29.01.2019.

Websites

China Law Translate. "China Law Translate." https://www.chinalawtranslate.com/en/our-team/, accessed January-May

Christensen, Jan Erik. "Lær kinesisk AS." https://www.laerkinesisk.no/, accessed 18.04.2019

Daum, Jeremy. "Who did China ban from flying?" https://www.chinalawtranslate.com/en/who-did-china-ban-from-flying/, accessed 30.04.2019

Human rights in China. "UN Treaty Bodies and China." https://www.hrichina.org/en/un-treaty-bodies-and-china, accessed 10.04.2019

JSTOR. https://www.jstor.org/,

Lawrence Livermore National Laboratory. "Laboratory and Norwegian researchers collaborate to improve cancer screening." https://www.llnl.gov/news/laboratory-and-norwegian-researchers-collaborate-improve-cancer-screening, accessed 26.02.2019

Oria, UiO:. https://www.ub.uio.no/,

University of Oslo. "Network for Asian Studies." https://www.sum.uio.no/english/research/networks/network-for-asian-studies/, accessed 15.01.2019

Whistler. https://whistlerapp.org/, accessed 02.04.2019

Other

Freedom House. "Freedom in the World 2018. Democracy in Crisis." 2018.

Future Thinkers Podcast. *Alex Gladstein: Anti-Authoritarian Technologices and The Future of Governance.* Podcast audio. Accessed 10.03.2019, 2019. https://futurethinkers.org/alex-gladstein-anti-authoritarian-technologies-and-the-future-of-governance/.

Hoffman, Samantha. "Social credit: Technology-enhanced authoritarian control with global consequences." Canberra: Australian Strategic Policy Institute, 2018.