The discontent of social scoring through state surveillance using the Chinese Social Credit system as a case study

Danielle van Zyl

Supervised by Dr Co Pierre Georg

University of Cape Town

Department of Commerce

In fulfilment of requirements for a Master's Degree

November 2024

Declaration of Originality

I, Danielle van Zyl (student number: VZYDAN020), hereby declare that this dissertation is entirely my own work, produced without assistance or collaboration with others, except where explicitly acknowledged. All sources of information and ideas have been duly cited and referenced in accordance with the conventions of academic citation.

This thesis/dissertation has been submitted to the Turnitin module (or equivalent similarity and originality checking software) and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor

Signed: Signed by candidate

Abstract

Many governments worldwide, particularly in democratic countries, are rapidly implementing surveillance technologies and expanding their surveillance programs, causing widespread concern. Although these governments claim to use this technology exclusively for ensuring safety and security of citizens, it has also facilitated unchecked control and power abuse by the state. The COVID-19 pandemic made many such abuses glaringly evident. Governments and private companies have partnered to create advanced surveillance programs that generate unprecedented amounts of personal data. This literature review explores the increased use and advancement of state surveillance systems worldwide and the extent to which citizens are identified and tracked. Social credit scoring systems are understood using the Chinese Social Credit Scoring System (CSCSS) as a case study. This paper evaluates the potential use of social scoring systems to enhance the state's surveillance capabilities to influence, control, and extend its power over citizens. The paper explores the current limitations of the CSCSS and analyses the creation of similar future systems in the West. State-controlled scoring systems can completely change the state's role in society, including how it governs and enforces legislation. Analysing the CSCSS highlights the difficulty of creating fair and integrated social credit systems that use incentive mechanisms to alter behaviour. The potential harms of a social credit system to citizens are vast. Concerns about individual privacy and the abuse of power are valid; however, the unfair treatment of minorities and the oppression of political opponents are additional concerns under algorithmic rule. Current regulation is insufficient to protect citizens' privacy as surveillance scoring programs become more far-reaching and invasive over time.

Contents

1 Introduction

We live in an age of surveillance (Richards, 2013) and algorithms (Loubere & Brehm, 2018). New technologies and methods, such as CCTV cameras, GPS tracking apps, and artificial intelligence (AI), increase the ability to track, observe, and monitor (Sætra, 2019). Sætra writes that the digital technologies that revolutionise our modern-day lives also create detailed records of almost every aspect. The scope and variety of the types of surveillance possible today are unprecedented in human history (Ünver, 2018). Information is collected systematically and indiscriminately and no longer on a need-to-know basis (Rubinstein et al., 2017). As surveillance technologies multiply, so too have the entities that wish to surveil (Lyon, 2019). Society commonly assumes that authoritarian and totalitarian regimes have repressive and extensive surveillance programs, but they are no longer the only governments with advanced surveillance programs (Ünver, 2018). Feldstein (2022) writes that democratically elected governments in the West have deepened their commitment to state surveillance and argues that this is especially concerning as more liberal democracies decay. Since the terrorist attacks in the early 2000s, anti-terrorism measures have been one the largest justifiers for state surveillance, but also a seemingly ever-growing list of other concerns (Richards, 2013). Richards writes that these concerns include public security, protecting children from predators, cybersecurity and intellectual property, and, in more recent years, epidemic management and containment for improved public health. As technology develops at an unhindered pace, so do the state's surveillance capabilities that encroach on privacy and freedom.

This literature review explores the history and troubling trends of state surveillance, examining the influence of technological advancements and the acceleration brought about by the COVID-19 pandemic. States no longer operate alone, as partnerships with private companies are common (Zuboff, 2019). This paper reviews empirical studies to identify factors influencing the acceptance levels of state surveillance, in particular the usage of Facial Recognition Technology (FRT). The Chinese Social Credit Scoring System (CSCSS) is currently the most advanced state-level social scoring system. It has been designed and built since the early 2000s, and its development has ramped up since 2014, with the Chinese Communist Party (CCP) issuing various implementation roadmaps.

Social scoring systems (SSS) represent the intersection of three global trends: the migration from human to digital decision-making, the shift from top-down regulation toward more sophisticated conceptions of governance, and the overwhelming belief in the power of big data and analytics to address virtually any problem (Werbach, 2022). Data-driven feedback incentives that shape behaviour are not unique to China (Creemers, 2018), and this paper explores the creation of similar programs in the West and the likely limitations. Surveillance might benefit society in some ways (Monahan, 2011), but it does not come without concern. Sinister ends are served through state surveillance as it empowers states to abuse their power (Sætra, 2019). In this context and throughout the literature review, 'abuse of power' refers to the inappropriate use of surveillance technologies by the state to exert excessive and unchecked control over citizens. This includes actions beyond ensuring safety and security, such as infringing on privacy, targeting minorities, oppressing political opponents, and extending state power in ways that undermine democratic principles and human rights (Feldstein, 2022).

The aim of this literature review is to gather and critically evaluate all relevant material on social scoring through state surveillance, with a particular focus on understanding the harms it may cause. By using the CSCSS as a case study, this review seeks to explore the practicalities and implications of implementing such a system. It aims to provide a comprehensive summary of various perspectives. Due to the secretive nature of state surveillance, especially concerning the CSCSS, it is challenging to obtain detailed data and information. This literature review strives to present a thorough analysis based on the available research despite these challenges.

2 State Surveillance

This section examines the history of state surveillance and how the COVID-19 pandemic acted as a catalyst for many governments to implement extensive surveillance programs (Kim & Kwan, 2021). It also highlights the role of private companies in advancing state surveillance capabilities through innovative technologies (Lyon, 2019). The section concludes with an empirical case study that explores citizens' willingness to accept state surveillance technology

Surveillance studies are diverse and, in some cases, inconsistent and ambiguous due to the definition of terminology (Steinfeld, 2017). Boersma et al. (2014) define the 'state' as an assemblage of individuals and organisations that draw a particular kind of authority in their activities. Further, Boersma et al. define 'surveillance' as "any collection and processing of personal data, whether identifiable or not, to influence or manage". Similarly, Richards (2013) defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". Both Boersma et al. and Richards' definitions of surveillance highlight that state surveillance has a clear and potentially sinister purpose - to analyse collected information and draw inferences from that information to influence and control.

State surveillance has expanded its scope to the routine and systematic collection of data (Ünver, 2018). In the state's quest to find all the needles in the haystack, it has opted to add more hay to the haystack.

2.1 Rise of state surveillance

State surveillance is commonly negatively associated with words such as 'spying' and 'espionage' (Boersma et al., 2014). A common historical belief is that individuals involved in criminal activity or political opponents are the primary targets of state surveillance. However, this is no longer the case as surveillance programs increase in scope and use (Feldstein, 2022). Surveillance technology has rapidly expanded from the cold war era wiretaps and hidden cameras to autonomous systems such as drones, satellites, and cyber surveillance (Westerlund et al., 2021). Until quite recently (the 2000s), surveillance has entered common parlance to describe an everyday part of people's lives rather than something extraordinary (Boersma et al., 2014). For example, CCTV cameras line the streets of many cities and cellular apps store GPS location data (Creemers, 2018).

The reality is that state surveillance has long been a part of society in different shapes and forms (Boersma et al., 2014; Nam, 2019). States have, over many years, built up surveillance infrastructure with the desire to keep a watchful eye over their citizens (Richards, 2013). Richards argues that state surveillance enables ruling parties' unfettered access and control of ordinary citizens by exploiting power dynamics. The unbalanced power dynamics seen explicitly in authoritarian and totalitarian regimes are becoming more present in democratic regimes (Jarman, 2021). Surveillance by the state has shifted from collecting information on potentially criminal individuals to passively monitoring

everyone (Feldstein, 2020). Some states even predict a person's chance of committing a crime before it occurs (Turner Lee & Chin-Rothmann, 2022).

2.1.1 History of surveillance

State surveillance has a long and complicated history; this paper will focus on a few main themes: identification systems, new technology, and surveillance culture. Identifying citizens in a country is inextricably linked to surveillance and is a crucial requirement for a state to monitor individual conduct (Sankar, 1992). Sankar argues that states need a legitimate and reliable record-keeping system to identify citizens individually. Identity cards (IDs) allow states to identify and store information about their citizens (Caplan & Torpey, 2001). Caplan & Torpey suggest that although state surveillance did not start with IDs, identification systems are a hallmark of modern states. Identification systems collect and store personal information such as an individual's first and last names, birth date, photos (Boersma et al., 2014), and biomedical data like fingerprints (Lyon, 2019).

In the USA, criminal record keeping started around the 1700s, with the state keeping information on a limited number of incarcerated prisoners (Sankar, 1992). Sankar writes that it was not until the first world war that the USA and European governments started requiring all citizens to partake in state-controlled identification programs. Sankar argues that before the 1900s, someone could live their whole life in a country without the government knowing anything about their existence.

Sankar asserts that IDs challenge civil liberties and human rights more than any other surveillance technology. Similarly, Haggerty & Samatas (2010) argue that the ID card system is one of the most intrusive instruments of surveillance societies. Boersma et al. (2014) acknowledge that IDs may be a form of surveillance that denies human rights but, in other contexts, be the 'giver' of human rights. Further, Breckenridge et al. (2012) write that ID systems are the acknowledgement of existence and identity, which forms a basis for human rights. Being able to identify citizens carries both positive and negative implications (Boersma et al., 2014). Boersma et al. highlight an example from history when the Nazis exploited the emerging IBM identity technologies during the Third Reich to identify Jewish individuals. More recently, the CCP has been discriminately targeting the Uyghur ethnic group in China's Xinjiang province (Loubere & Brehm, 2018). Between 2017 and 2018, growing numbers of re-education camps detained over 12% of the adult Uyghur population (BBC News, 2022).

In Higgs' (2004) book, *'The Information State in England: The Central Collection of Information on Citizens since 1500'*, Higgs contends that Britain did not emerge as a surveillance state due to security or terrorism concerns. Instead, Higgs attributes it to Britain becoming a welfare state. Higgs asserts that the surveillance practices in a welfare state typically have more extensive reach because people often overlook and underestimate them, and they have lingering impacts. As evidence, Higgs points to an example where social welfare workers accumulate substantial amounts of detailed personal data about children and families over an extended time.

The advancement of technology and information systems is essential when considering the state's increased surveillance measures and intrusiveness (Feldstein, 2020). Advancements in data storage, data collection, predictive modelling, AI, and identification of individuals through voice, facial, and biological data massively enhance the capability of surveillance systems (Feldstein, 2022). However, Boersma et al. (2014) argue that it is overrated to focus on improved technology as the main driver for increased state surveillance. Lauer (2012) supports Boersma et al.'s argument by stating that the advent of camera and telegraph technology sparked as much concern as today's new technologies do. Observing and documenting others is age-old human behaviour, and social practices influence surveillance (Boersma et al., 2014; Nam, 2019 ; Monahan, 2011). Haggerty & Samatas (2010) write that effective state surveillance does not need to be advanced. They suggest that some of the most repressive forms of state surveillance used by many authoritarian countries were not advanced at all. Haggerty & Samatas argue that a culture of fear and suspicion in society is much more powerful than any surveillance technology.

2.1.2 Troubling Surveillance Trends

States are adopting advanced surveillance technologies that are highly intrusive (Kampmark, 2014), flawed and poorly understood (Wong, 2020). The 9/11 terrorist attacks were a notable turning point for increased state surveillance programs, with the US government exponentially increasing its counter-terrorism spending after 2001 (Lum et al., 2006). The enhancement of digital technology acts as an enabler for state surveillance programs and augments state powers in many ways (Feldstein, 2022). Surveillance technology poses a threat to free expression and the rule of law (Feldstein, 2022), and it also brings up concerns about oversight (Ünver, 2018). Snowden revealed the unprecedented scope

and size of state surveillance in the USA and its allied countries (Rubinstein et al., 2017). Snowden's release of approximately 50000 pages included revelations about the NSA's warrantless wiretapping of telephone conversations in real-time (Foreign Policy, 2013).

Surveillance technology has vastly improved and comes in all forms, from drones, facial recognition cameras, GPS location devices, satellites, and RFID tags (Kostka et al., 2023; Ünver, 2018). Surveillance tools have become more affordable as large-scale commercial technology matures (Zhang et al., 2021). AI technology and computers extend states' power to monitor citizens due to the enhanced ability to collect and analyse large quantities of data (Feldstein, 2022). The automation of work through machines has expanded the scope and scale of surveillance programs, freeing states from limitations on citizen monitoring imposed by workforce size (Pozen, 2016). Ünver (2018) argues that AI technology and improved data storage enable states to capture unprecedented amounts of personal information, flag perceived anomalies, and attempt to predict future events. An increasing amount of police departments in the USA rely on facial recognition technology (FRT) to facilitate arrests, charges, detentions, and criminal convictions (Wong, 2020). Wong writes that the New York Police department had made over 3000 arrests using FRT within the first few years of use.

Western and Eastern countries often have different political ideologies affecting surveillance's pace, extent, and citizen approval. While established autocracies eagerly utilise the latest surveillance tools, the rise in the use of state surveillance tools by liberal states is of even greater concern (Feldstein, 2022). In the Feldstein's 2022 report, *'The Global Struggle Over AI Surveillance: Emerging Trends and Democratic Responses'*, 54% of countries classified as 'more democratic than authoritarian', were identified to have known AI surveillance capabilities. Further, in swing states (states identified with serious democratic weaknesses and concentrated power), 66% had known AI surveillance programs. The report argues that the adoption rate of AI technology will increase over time as the global level of democracy backslides, raising various concerns.

States struggle to balance freedom, privacy protection, and public order (Pozen, 2016). In India, the world's largest democracy, the police used facial recognition devices to screen protestors entering a protest venue and used surveillance drones to oversee protesting activities (Feldstein, 2022). In the USA, the FBI used FRT to identify and confirm suspects' identities in the Capital Riot attack of 2021

(Vincent, 2021). Vincent writes that images from the Capital Riot suspects were run through the web to identify them, linking the suspects' images to their social media accounts and other public information. Predictive policing, used to predict future crimes, is currently being widely used in Western Europe (the UK, Germany, Spain, Switzerland, and France) as well as in the Americas and Asia (Piotrowicz, 2019). In 2018, the Pakistani government bought an $18.5 million web-based monitoring system that would monitor communications data on behalf of the country's telecoms regulator (Feldstein, 2022).

2.2 COVID-19 was a catalyst for state surveillance

The emergence of the COVID-19 pandemic in late 2019 marked the most significant and critical global health crisis to date (Kim & Kwan, 2021). Eck & Hatz (2020) argue that the rise of state surveillance is an unexpected by-product of the pandemic as states undertook unprecedented measures in monitoring citizens and censoring or manipulating information. To save lives, states were willing to forgo privacy concerns by implementing varying levels of surveillance and pervasive control measures (Ioannou & Tussyadiah, 2021). According to Eck & Hatz (2020), the measures taken by many states worldwide during the pandemic are akin to tactics used to curtail domestic political threats. Surveillance vendors globally experienced a boom in sales, with governments and private companies developing more sophisticated surveillance tools to suppress the COVID-19 outbreak (Feldstein, 2022).

Gershgorn (2020) states that during the first few months of the COVID-19 pandemic, more than 34 countries (of which 22 were full democracies) enacted surveillance measures on their citizens. Some examples of pandemic containment surveillance measures include track and trace programs leveraging mobile applications (Boudreaux, 2020), censoring fake news across social media and news outlets, and storing extensive amounts of personal and biometric information (Kampmark, 2020).

Track and trace containment measures are particularly concerning as individual geo-location data is used for both preventive and quarantine adherence purposes (Boudreaux, 2020), even though its efficiency in curbing the spread of the virus is questionable (Eck & Hatz, 2020). Eck & Hatz write that the track and trace apps of Norway, Bahrain, and Kuwait were described as one of the most invasive in the world by Amnesty International. According to Gershgorn (2020), the Iranian government launched an app and urged its citizens to use it for self-diagnosing COVID-19. However, it ended up storing the location data of Iranians. Hong Kong and Bahrain required travellers to the country to wear electronic

tracking bracelets; synced to the individual's cell phones (Miyamoto, 2020). Many countries issued COVID-19 passes, others called citizens to check on their adherence to isolation measures, and others used credit card purchase data to identify where individuals were at certain times (Kim & Kwan, 2021). The USA and China had very different responses, mainly due to political and cultural differences. In the USA, citizens objected to wearing masks, while Chinese citizens faced complete lockdowns where they could not leave their homes for food.

Censoring measures were also very concerning during the pandemic as governments responded to the rapid outpouring of misinformation on social media (Feldstein, 2020). Many governments introduced the criminalisation of spreading fake news as they tightened their information control (Eck & Hatz, 2020). Eck & Hatz argue that by the end of 2020, twenty-four countries passed laws punishing the dissemination of fake information, with fifteen countries introducing prison sentences. Further, Eck & Hatz write that many autocratic countries adjusted their existing information control filters. Other countries such as Armenia, introduced laws mandating the Prime Minister's office as the only source of truth for COVID-19 information. The Chinese state deleted posts, user accounts, and hashtag trends during the start of the pandemic when users started posting about a mysterious disease in Wuhan (Eck & Hatz, 2020).

Not only did governments mandate the collection of personal information, but individuals also freely shared sensitive details about themselves (Wang, 2021). Wang argues that during the pandemic, individuals started revealing personal health information that they wouldn't have previously shared, such as their travel history, symptom description, test findings, and medical history.

The COVID-19 pandemic fundamentally changed how individuals interact, work, and play (Jarman, 2021). The pandemic promoted the increased development and use of online services such as e-commerce, eLearning, virtual healthcare services, and social media (Wang, 2021). During the heart of the pandemic, social media platforms like Facebook and Instagram saw over a 61% increase in usage (Nabity-Grover et al., 2020). Further, Nabity-Grover et al. state that the usage of Chinese communications platforms, WeChat and Weibo, increased by 58%. The increased use of online services raise concerns about personal information protection and freedom of speech (Steinfeld, 2017). Many coun-

tries relaxed their regulation restrictions and cooperated with private companies to collect information on behalf of the state in their quest to manage the COVID-19 outbreak (Wang, 2021).

Kampmark (2014) states a major worry: surveillance and control measures continue to exist even after they've served their initial purpose. In response to the 9/11 attacks, the USA government introduced the Patriot Act of 2001, giving the state extensive surveillance powers with limited supervision (Eck & Hatz, 2020). Some of these surveillance powers included allowing the state to access citizens' telecommunication information without a court order (Gershgorn, 2020). This act is still in place in the USA, long after the 9/11 terrorist attacks, and is an example of governments using surveillance powers long after their intended purpose. In response to protests triggered by banks freezing customer deposits in June 2022, suspicions arose that authorities in the Chinese province of Henan were using China's health code app, initially designed as a pandemic tool but still in use after the pandemic, to restrict some customers' movements (Wong & BBC Chinese, 2022).

2.3 Intermingled private and state surveillance

State surveillance tools are no longer just created and managed by the state (Fuchs, 2019). Governments and non-government entities support each other in complex manners that are often impossible to disentangle (Richards, 2013). The Snowden revelations also affirmed the deep cooperation between the state and private companies in sharing personal information (Steinfeld, 2017). The NSA subcontracts surveillance to over 2000 private security companies (Fuchs, 2019). Private companies have vastly improved the quality and reach of surveillance tools, and many companies collect personal data similar to those required by police or intelligence agencies (Boersma et al., 2014). Increased privatisation of public services created what Steinfeld (2017) calls 'economic surveillance', where surveillance penetrates the commercial realm. In Zuboff's 2019 book: *Surveillance Capitalism*, Zuboff likewise argues that state surveillance has moved into the commercial sphere with collaborative arrangements between the state and companies.

Private companies have created software and hardware for governments to surveil citizens, including FRT and spy satellites (Feldstein, 2022; Kostka et al., 2023). Chinese companies are at the forefront of providing surveillance technologies to many states worldwide. The Chinese state subsidies Chinese companies, making them particularly successful and competitive (Feldstein, 2022). Feldstein (2022)

states that Chinese companies such as Hikvision and Dahua account for around 40% of all surveillance camera sales, whilst an article by Research Markets (2022) states that the market share was around 60% in 2022.

In many cases, autocratic regimes are the biggest buyers of surveillance technology, but recently more democratic states such as Poland, Hungary, India and the Philippines have invested in surveillance technology (Feldstein, 2022). Feldstein (2022) writes that states with more money than others are careful not to partner with a single company but to spread their surveillance partnerships between multiple companies. For example, Feldstein (2022) writes that Saudi Arabia uses private companies such as Huawei, Google, Amazon and Alibaba to enhance its surveillance technology. A big concern is private companies' collection of personal data and the state's ability to use or purchase the data (Feldstein, 2020). States have varying degrees of accessing private-held data, but in many cases, they can purchase individual movement data without probable cause from data brokers (Turner Lee & Chin-Rothmann, 2022). The US government requested data from Apple, Facebook, Google, and Microsoft over 112,000 times during the first five months of 2020, with an 85% success rate. Many successful data requests did not need an approved court order (Turner Lee & Chin-Rothmann, 2022).

Clearview AI is an example of a company that governments worldwide collaborate with for their facial recognition surveillance programs (Turner Lee & Chin-Rothmann, 2022). Turner Lee & Chin-Rothmann write that the company scrapes publicly available images from social media sites and websites and stores them in an extensive database. Clearview AI then matches those images to others with similar characteristics without the individual's knowledge. Clearview AI allows its customers to upload images of individuals in its database, giving the customer links to the websites and profiles of the matching individual. As of April 2022, Clearview AI had over twenty billion images and had helped over three thousand law enforcement agencies in the US to identify individuals not found in the FBI's database of about six-hundred-and-forty million images (Turner Lee & Chin-Rothmann, 2022). Governments collaborated with private companies during the COVID-19 pandemic to curtail the spread of fake news (Eck & Hatz, 2020). Eck & Hatz write that companies such as Facebook, Twitter, and Google used algorithms to remove posts they deemed fake news and removed events from their sites that contravened social distancing rules.

According to Loubere & Brehm (2018), Landasoft, a private Chinese defence company, teamed up with the Chinese state to become part of China's Integrated Joint-Operations Platform. This collaboration aimed to enable mass surveillance of minority groups in Xinjiang, China. Loubere & Brehm explains that Landasoft developed an extensive police database that gathers surveillance and personal information, including DNA, relations with family and friends, movement data, package delivery data, and electricity usage. Loubere & Brehm state that, ultimately, this data is used to assign public safety scores to individuals and flag suspicious individuals to authorities. If an individual is deemed suspicious, they are often detained and sent to re-education centres.

2.4 Willingness to accept state surveillance measures

Citizens' willingness to accept intrusive state surveillance measures encroaching on privacy is very dependent and situational (Pozen, 2016). Ziller & Helbling (2021) argue that surveillance programs' necessity, transparency, and extensiveness greatly influence citizens' perceptions. Westerlund et al. (2021) argue that the Edward Snowden leaks and the COVID-19 pandemic are critical events that triggered renewed debate and media attention around state surveillance policies. Ioannou & Tussyadiah (2021) write that increased levels of anxiety and worry about the potential negative consequences of surveillance occurred after the 9/11 attacks and the Snowden leaks. Steinfeld (2017) argues that support for state surveillance is much higher compared to surveillance conducted by companies.

Many states have increased the scope of surveillance programs, partly because of the advancement in technology and reduction in IT costs, but more popularly due to increased threats of terrorism and domestic security concerns (Ziller & Helbling, 2021). States have found themselves in predicaments as many citizens view them as responsible for domestic security, similarly, to controlling inflation or running welfare programs (Ünver, 2018). Ünver writes that, generally, there are political repercussions for states not seen as doing enough to protect citizens from domestic and international security threats. Hence, citizens generally welcome policies aimed at ensuring public security. The critical debate is how states can ensure public security whilst protecting rights (Ziller & Helbling, 2021).

Salient threats to public safety (real or perceived) increase the support of far-reaching surveillance programs (Wang, 2021). Acts of terrorism are sporadic when looking at the number of deaths and injuries caused. Six people have died each year in the US due to terrorist attacks since 9/11, substan-

tially less than the number of people dying from bathtub drownings (Jarvis, 2022). Jarvis concludes that terrorism is so rare outside of war zones that it is statistically insignificant and could very easily pass as not existing. Nevertheless, terrorism invokes fear in many individuals to the extent that they would sacrifice their liberties for perceived or improved security - albeit irrationally. The effectiveness of counter-terrorism measures also comes into question. A systematic review of seven studies on counter-terrorism programs indicated that not only did the counter-terrorism programs not achieve their desired outcomes, but in some cases, the counter-terrorism programs increased the likelihood of terrorism occurring (Lum et al., 2006).

Wang (2021) states that studies have found that people are more willing to sacrifice personal information and privacy if observable benefits exist. Wang argues that the COVID-19 pandemic is an example of citizens willingly sharing much more personal information with the state and private companies than they usually would have. Disclosing information during the pandemic was not just about receiving detailed health care or pre-diagnosis. Many citizens willingly shared personal information in light of a perceived public good.

Steinfeld (2017) mentions a prevalent argument supporting state surveillance: "If you have nothing to hide, you should not be concerned". The argument rests on the premise that the average individual is unimportant to the state and that no harm will come from being surveilled. In Glenn Greenwald's 2014 Ted talk on: *'Why privacy matters'*, he argues that this type of reasoning is problematic for privacy issues (TED, 2014). Glenn argues that every day, people decide what information they share with others and what they do not want to share. For example, not wanting to share the news about purchasing a new house with work colleagues does not mean someone is hiding something terrible. Glenn maintains that choosing what information remains private and what gets divulged is a critical aspect of human liberty.

Liu (2023) and Ziller & Helbling (2021) both express concern over corporate and state surveillance becoming a prominent aspect of life in the modern world. Surveillance is so rooted in daily life that we now live in a surveillance society, leaving few areas of life still private (Westerlund et al., 2021). This ubiquitous use of surveillance in the modern day raises questions about the relevance of citizens' consent.

2.4.1 Empirical study: attitudes toward Facial Recognition Technology (FRT)

Governments are increasingly adopting FRT to enhance public services and law enforcement. In a study examining public attitudes toward FRT, Kostka et al. (2023) explored the support of FRT usage in the public sphere through online surveys and semi-structured interviews involving citizens from China, Germany, the United Kingdom, and the USA. The acceptance level results amongst the four countries are indicated in Figure 1 below, showing varying levels of acceptance, with China exhibiting the highest (51%) and the USA and Germany lower (37% and 38%, respectively). Opposition to FRT was lowest in China (22%).

In the study, respondents were asked about public issues—violations of rules, socially unacceptable behaviour, and security threats—to gauge their impact on FRT acceptance. Figure 2 reveals that, notably, crime was the top concern across all four countries, while terrorist threats ranked second highest in all countries except China, where it ranked second to last. Intriguingly, crime concerns were not significantly linked to FRT acceptance, but concerns about terrorist threats correlated with increased public support for FRT, emphasising contextual influences.

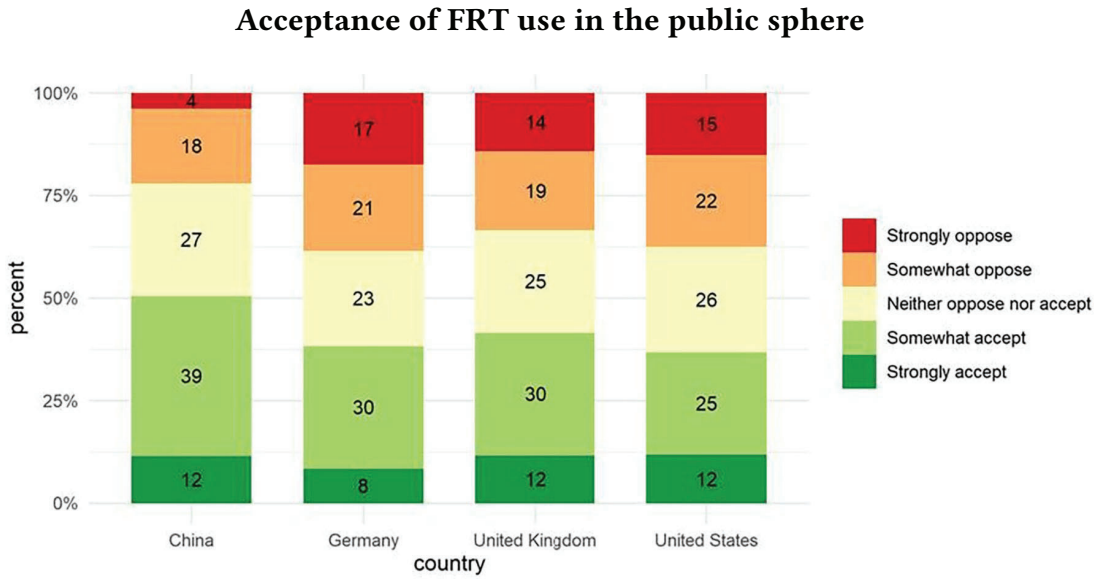

Figure 1: The stacked bar plot depicts acceptance levels of Facial Recognition Technology (FRT) across four studied countries. In China, 51% of respondents strongly or somewhat strongly accepted FRT, whereas Germany showed the strongest opposition (Kostka et al., 2023).

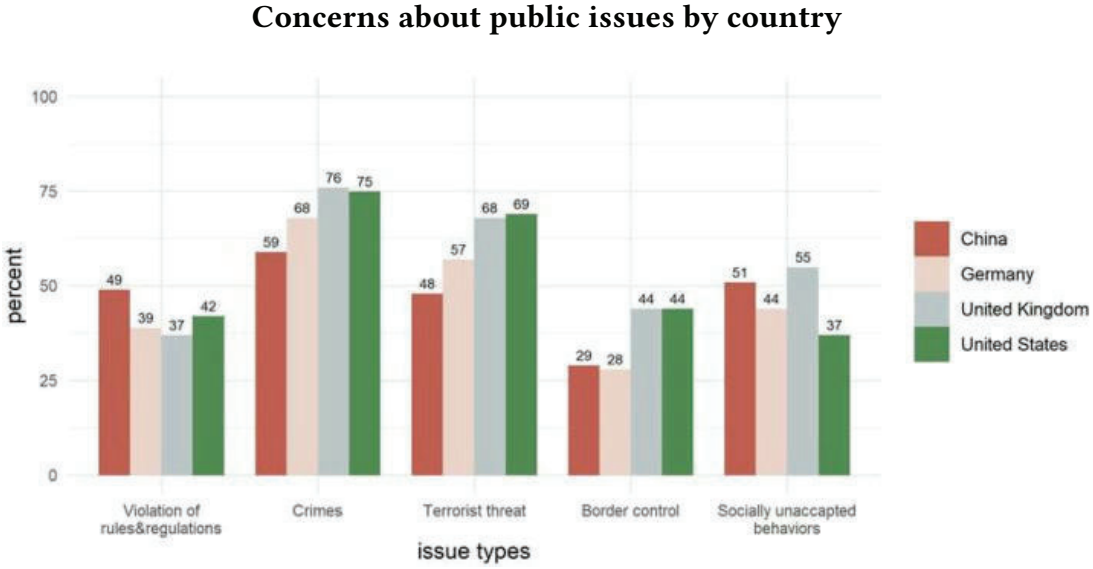

Figure 2: The grouped bar chart shows survey respondents' varying levels of concern on five public issues influencing Facial Recognition Technology (FRT) across countries, highlighting crime as the foremost concern universally, while notably, the study found no significant correlation between crime concerns and FRT acceptance (Kostka et al., 2023).

Kostka et al.'s study also identified that individuals' privacy preferences and technology-related traits strongly influence their acceptance of FRT in public use. Privacy concerns emerged as the most significant factor negatively impacting acceptance levels. Notably, a substantial portion of respondents (41%) believed that FRT led to privacy violations in a general sense. However, when asked specifically about their own individual privacy later in the survey, only 25% perceived FRT as a threat to their personal privacy. Importantly, concerns about privacy, whether in a general or individual context, consistently correlated with lower FRT acceptance across all four countries, challenging the notion that Chinese citizens are indifferent to privacy concerns. These findings align with previous research on 'contextual integrity,' emphasising that various contextual factors, including socio-political beliefs and norms, influence citizens' calculations of privacy risks and benefits (Nissenbaum, 2004).

3 Case Study: The Chinese Social Credit Scoring System

This section provides an overview of the current CSCSS, including its history, operations and limitations. The CSCSS is used as a case study to understand how state social scoring systems can be used as an extension of state surveillance programs.

Mike Pence described the CSCSS in a 2018 speech as an Orwellian nightmare aimed at controlling virtually every facet of human life (Horsley, 2028). News articles by Western media outlets, such as those published by the Economist, argue that only the CCP could create and implement such a nefarious and perverse system (Loubere & Brehm, 2018). Westerners often compare the CSCSS to the dystopian episode "Nosedive" in the hit Netflix series Black Mirror, which showcases people's lives in a socially scored society (Wired, 2019). In the episode, individuals score their interactions with each other out of five, which in turn, determines their socio-economic status. Liu (2023) and Loubere & Brehm (2018) argue that the CSCSS is not as advanced nor uniquely Chinese as has been portrayed by Western media, Although the CCP is secretive and accurate information on the CSCSS is scarce, official documents for the CSCSS have not mentioned creating a unified score for each citizen (Horsley, 2028). Drinhausen & Brussee (2021) argue that the CSCSS focuses on the documentation and tracking of legal compliance by creating comprehensive digital files. They contend that although the CSCSS is a powerful program in the hands of an authoritarian government, many other CCP programs are much more concerning than the CSCSS. In contrast, Loubere & Brehm (2018) argue that social scoring systems such as the CSCSS will sit at the centre of oppressive and invasive surveillance regimes. Some scholars contend that the West's apprehension about CSCSS mirrors their own countries' worries about the escalating surveillance powers of states and private corporations (Schroeder, 2022).

This section provides an overview of the current CSCSS and its limitations. The CSCSS is used as a case study to understand how state social scoring systems can be an extension of state surveillance programs.

3.1 Overview of the Chinese Social Credit Scoring System

'Social credit' is generally used in China to reflect a range of meanings, from financial creditworthiness to broader meanings such as trustworthiness, honesty, integrity, and socially acceptable behaviour

(Drinhausen & Brussee, 2021). However, Drinhausen & Brussee argue that the term is not clearly defined, and its vagueness has allowed unrelated policies to fall under the catchphrase. The first high-level political mention of the CSCSS was during the 2002 Party Congress (Creemers, 2018). The first blueprint drafts of the system distinguished it from Western counterparts by referring to the system in the context of creditworthiness and to a broader notion of honest and trustworthy market conduct (Hoffman, 2019). A key turning point in the development of the CSCSS was during the 2014 4th Plenum, where the Chinese state published a high-level policy document detailing the creation and implementation plans for the CSCSS by 2020 (Knight, 2023). In Jan 2021, the CCP issued a renewed 5-year roadmap for the CSCSS, highlighting its importance in supporting the legal and administration system (Drinhausen & Brussee, 2021).

The CSCSS today is a policy framework for a state-run social credit system that combines fragmented, localised initiatives that share a set of objectives and principles (Creemers, 2018). Creemers argues that it is a system underpinned by an incentive mechanism, where actors are rewarded or punished based not only on the lawfulness of their actions but also on the morality of their actions. The CSCSS is a product of many events that have shaped Chinese culture and politics, most notably China's vast economic growth from the 1970s (Drinhausen & Brussee, 2021). Drinhausen & Brussee write that the purpose of the system has evolved and expanded from initially developing the Chinese financial services industry to increasing trust within society, improving the enforcement of regulation and existing laws, as well as the improvement of state governance.

The initial need for the CSCSS came from a series of market reforms to stem certain ills in Chinese society, such as a perceived lack of trust in society and the state (Creemers, 2018). During the 1970s, food safety scandals, labour law violations, and environmental scandals eroded trust within Chinese society. Creemers argues that a lack of supervisory market actors contributed to the mistrust of the government. The 2008 Melamine scandal, which resulted in over 54,000 hospitalisations of children due to infant formula milk containing Melamine, received significant backlash in China and worldwide. The infant formula contained Melamine, increasing the amount of nitrogen in the formula, which allowed the formula to appear to pass protein standards (Creemers, 2018).

Further, the CSCSS is a response to a moral crisis in the state, observed during the second half of the Hu Jintao administration, where many state functions were localised, and rampant corruption weakened the perceived power of the central state (Creemers, 2018). The CSCSS is part of Xi Jinping's vision for improved governance, where data-driven governance can modernise and reshape the current fragmented authoritarian model (Loubere & Brehm, 2018).

Chinese culture and the state's role are fundamental considerations for the scope of the CSCSS, as moralistic terms are the system's foundation (Creemers, 2018). Creemers claims that a common belief in China is that every citizen contributes to society's harmony and that citizens must behave appropriately in public and civil structures. Further, Creemers argues that Chinese citizens expect the state to be a promoter of moral virtue. Hence, citizens believe that the state's role is to enforce laws and foster an environment of social morality. Drinhausen & Brussee (2021) argue that the idea that society can be controlled and engineered through a holistic approach that blurs the boundaries between state and society, public and private, forms the foundation of an SSS. In agreement, other scholars argue that the CSCSS is one of many examples of a more recent collective notation to increase transparency, accountability, and connectedness in society (Loubere & Brehm, 2018).

3.1.1 Workings

The CSCSS is not a single state-wide system that contains a central repository of scores and data (Li & Kostka, 2022). Instead, it is a fragmented system that encompasses various localised programs (Drinhausen & Brussee, 2021). Forty-seven institutions with partly conflicting intentions are shaping the system. These include the State Council as cross-ministerial coordinator, the National Development and Reform Commission (NDRC), and the People's Bank of China in the lead. Many institutions are responsible for implementing the system by establishing and managing platforms to track "social credit" in their respective policy fields (Drinhausen & Brussee, 2021). Due to the decentralised nature of the CCP, the CSCSS is a policy framework with a guiding set of principles. The CSCSS give local governments a mandate to create and implement a policy version based on their interpretation of the guiding principles and within the confines thereof. Forty-three local governments have built pilot systems since 2014, and twenty-eight model cities were identified in 2018 to test the implementation

of a nationwide system (Drinhausen & Brussee, 2021). Local governments have focused on different industries and have implemented different incentive mechanisms (Loubere & Brehm, 2018).

The Joint Punishment system is a significant program of the CSCSS outlined in the 2014 4th Plenum five-year plan (Creemers, 2018), which rests on a Chinese principle: "Once proven untrustworthy, restrictions should apply everywhere" (Drinhausen & Brussee, 2021; Knight, 2023) . The Joint Punishment system is a plethora of 'blacklists' that publicly name and shame offenders. Moreover, Creemers (2018) and Horsley (2028) argue that the public naming and shaming of offenders have added a 'reputation mechanism' to the system, which aligns with the 'incentive mechanism'. Hence, citizens and companies are financially and reputationally incentivised not to misbehave or act unsocially.

Each blacklist focuses on a critical industry, such as 'Food and Safety' or 'Energy, Industry, & Construction', and each list is relatively standardised. The most common blacklist target area is judgment defaulters - individuals and companies that do not abide by judgments handed down by Chinese courts. 70% to 90% of blacklists focus on judgment defaulters (Drinhausen & Brussee, 2021). Drinhausen & Brussee argue that blacklists affect a small section of the population, with companies being worst hit (1-2%), then individuals (0.15%-0.3%), and lastly, government entities (<0.1%). Further, policy documents on the CSCSS between 2003 and 2020 indicate that the leading target group for the blacklists are companies, with companies being mentioned around three-quarters of the time, compared to individuals just 10% of the time. Creemers (2018) mentions that the blacklist system blocked over nine million plane ticket sales and over three million rail ticket sales by March 2018. Most companies have a social credit file that combines basic information, such as founding dates, owners, and scores, with other credit information, such as penalties received, irregularities, and blacklist information (Drinhausen & Brussee, 2021). Chinese national courts manage the blacklists relatively effectively. Presently, blacklists only contain state and regulatory authorities' data (Creemers, 2018).

Local governments have also expanded the blacklist system to address local requirements and have created points-based credit rating systems with different incentive mechanisms (Li & Kostka, 2022). The 2016 Wuhan pilot program had a points-based rating system between 0 and 100. The rating system focused only on punishing severe cases of untrustworthiness (Drinhausen & Brussee, 2021). Comparatively, Drinhausen & Brussee write that the Jiangsu province program had points between

0 and 12, with varying levels of punishment. The punishment included an increase in electricity costs for relatively minor offences. Most of the programs are voluntary, with low active participation, and Drinhausen & Brussee argue that the programs are rudimentary, resembling incentivised loyalty programs like those created by airline companies. Only 5% of residents in the Xiamen province and 15% of residents in the Hangzhou province participated in the local state-run scoring systems (Li & Kostka, 2022). An analysis by Li & Kostka on semi-structured interviews indicated that participation in social credit systems was low for various reasons. The perceived effort to register and participate in the program was the most significant contributor to low participation (92% of respondents agreeing). Other reasons for low participation include having limited awareness of local programs (85% of respondents agreeing), concerns around privacy, the consequences of score reductions, and limited benefits. Werbach (2022) writes that the most popular benefit for individuals with high scores in the city of Xiamen was the ability to borrow library books for free. Authorities have since discontinued many local government programs and have banned punishments for low scores or minor transgressions like jaywalking (Drinhausen & Brussee, 2021).

Localised government-run 'social credit scoring' programs differ from private company programs. Private company initiatives such as Sesame Credit (owned by Ant Group Financial) are often incorrectly associated with the CSCSS. The CEO of Ant Financial, Lucy Peng's principled view on the role of Sesame Credit appears to align with the CCP. Lucy mentioned that Sesame Credit 'will ensure that the bad people in society do not have a place to go, while good people can move freely and without obstruction' (Loubere & Brehm, 2018). Sesame Credit uses data from Alibaba platforms and combines credit information with behavioural information (derived from a person's consumer behaviour and donating history), personal information (the extensiveness and reliability of personal information), social information (e.g., the quality of one's social network) and financial information (one's private assets, income and ability to pay off debts) to create a Sesame Credit score between 350 and 950 points (Creemers, 2018).

In contrast, state-run programs appear only to use state-acquired data. Creemers mentions that users with high Sesame Credit scores could receive benefits from Alibaba and its partners, such as fast-tracked visa applications and reduced deposit sizes for car rentals and hotels. Creemers writes that many people advertised their Sesame Credit score on Alibaba's dating app Baihe. Private scoring

programs, such as Sesame Credit, are now intended to only work as loyalty/reward programs due to the revoking of their pilot credit scoring licenses in favour of a unified credit scoring bureau named Baihang (Loubere & Brehm, 2018). Concerns about conflicts of interest and data accuracy forced Tencent's version of a credit scoring system to shut down one day after launching (Creemers, 2018).

3.1.2 The Flexibility of the System

The CSCSS is flexible as it keeps adapting to new priorities, which aligns with the National Development and Reform Commission's (NDRC) idea of an 'issue-focused government' (Drinhausen & Brussee, 2021). Figure 3 below showcases the changing policy priorities from 2003 to 2020. 'Food & Drug safety' was the main priority from 2003 to 2007, and then 'Energy, industry & construction' and 'Finance' were the main priorities until 2016. Since 2018, priorities seem to be more balanced, with a shift in focus to environmental protection. The rapid response to the COVID-19 pandemic highlights the flexibility and adaptability of the CSCSS (Drinhausen & Brussee, 2021). Drinhausen & Brussee write that local CSCSSs quickly deployed new sanctions and rules to enforce pandemic containment measures, requiring the correct travel history documentation and forced temperature readings. Further, the CSCSS helped ensure a safe and orderly return to workplaces, and blacklists considered debtor grace periods to accommodate the financial strains of the pandemic.

Chinese Social Credit Scoring System (CSCSS) regulation targeting various sectors and issues (2003 - 2020)

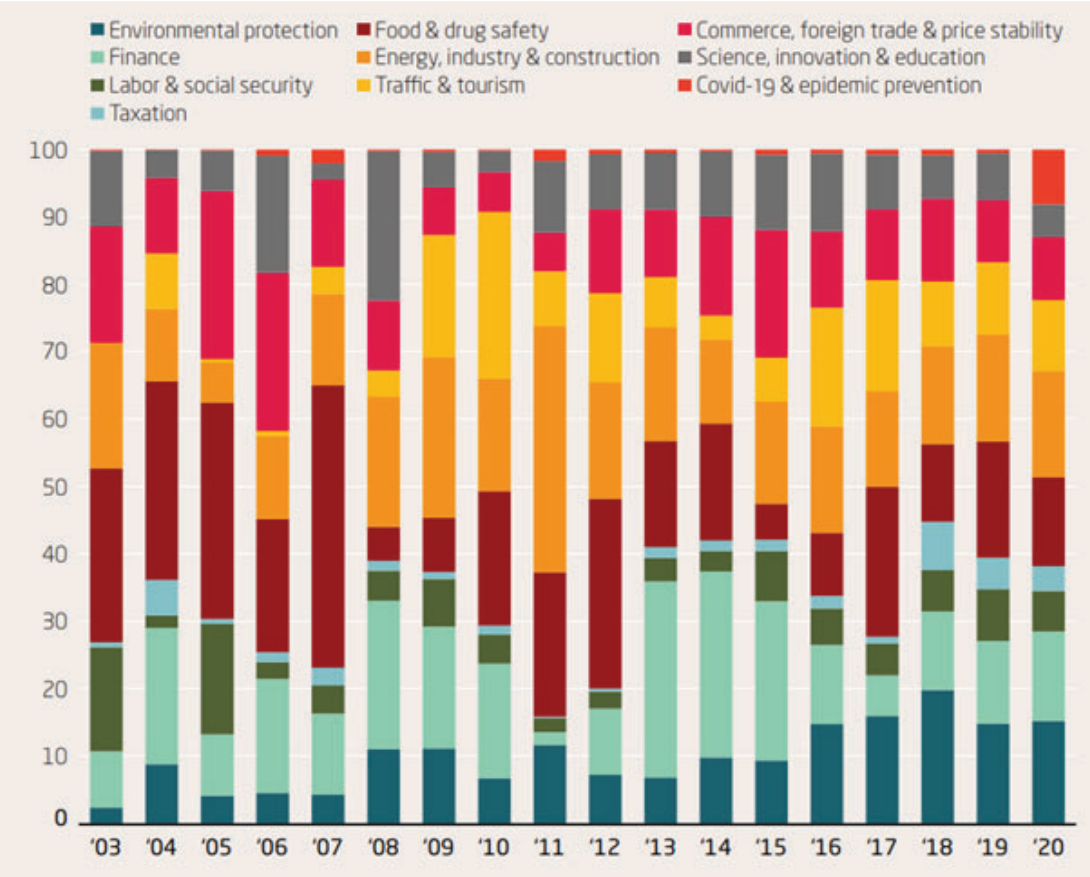

Figure 3: The stacked bar plot displays the evolving priorities of the Chinese Social Credit Scoring System (CSCSS) with *proportionate split* on the y-axis and *year* on the x-axis. A steady increase in environmental protection regulation and a notable decrease in financial regulation since 2015 is observed. (Drinhausen & Brussee, 2021).

3.2 Limitations of the Chinese Social Credit Scoring System

The current CSCSS has, in many ways, fallen short of the state's initial blueprints of the system. The system's new five-year plan (2021-2025) intends to mitigate some identified issues (Knight, 2023). These issues include inconsistent implementation, manual inputs, poor system integration, fragmentation, unclear boundaries, and corruption.

Given the localised implementation of the CSCSS, local governments implemented tailored versions of the system, highlighting its adaptability (Knight, 2023). However, it also created challenges around consistency and perceived fairness. A blacklist issued by the Wuhan model city in 2019 included some citizens on the list owing as little as 600 CYN (around R1500) (Drinhausen & Brussee, 2021). Drinhausen & Brussee write that this is in stark contrast to others owing millions or even billions of CNY. The disproportionate punishments concern individuals and companies, and the state council has been keen to address these issues. In 2021, the State Administration for Market Regulation issued a new draft policy clarifying the meaning of dishonest conduct. The draft policy mentions that for a severe offence classification, a law violation and either a marketplace discrepancy or a serious public safety threat must occur (Drinhausen & Brussee, 2021).

Another issue with the CSCSS is that the scope of what falls under 'social credit' is unclear because it has become an arbitrary term (Drinhausen & Brussee, 2021). For example, during the pandemic, some states blacklisted citizens for not wearing a mask, and the Anqing model city blacklisted a citizen for posting a video of an ambulance picking up another citizen - citing that causing 'public panic' was not allowed. Another example, which caused a public outcry in 2020, was when a nine-year-old child was placed on a blacklist due to the bad debts of her deceased father (Werbach, 2022). Some Chinese media outlets have criticised the unclear scope of the system. The Chinese state has taken steps to address the ambiguity of 'social credit' by drafting a new Social Credit Law to establish best practices and principles. The new law draft is still in progress, and Drinhausen & Brussee argue that it may take many years to implement state-wide legislation.

The localised implementation has introduced fragmentation issues, and many key data sources for the CSCSS do not feed into each other (Werbach, 2022). According to Drinhausen & Brussee, sharing local blacklist records with the national blacklist database is uncommon, with only 10% to 25% of lists shared. They write that even the shared blacklists are often not fully complete. Drinhausen & Brussee mention an example of a company that had committed a severe offence included on only one blacklist but not on other relevant ones. The fragmentation issue is further enhanced by the CSCSS being one of China's least digitised systems (Drinhausen & Brussee, 2021). The current CSCSS is very manual and relies on human investigation and decisions. There appears to be an onus on companies and individuals to check the lists for human error and incorrect placement on lists.

The CSCSS has come under scrutiny by Human Rights Watch for the perceived inability of individuals to appeal their inclusion on blacklists and for their prompt removal from blacklists once repaying debts (Drinhausen & Brussee, 2021). Further, Creemers (2018) mentions the inclusion of political opponents of the state in blacklists without proper notification and apparent recourse to appeals procedures. An investigative journalist, Li Hu, has maintained that he was incorrectly placed on a blacklist on a phantom claim and argued that the CCP is using the CSCSS to punish dissidents (Werbach, 2022). Creemers mentions that the National Development and Reform Commission (NDRC) identified the need to address these issues and argues that running a complex system like the CSCSS without mistakes would be a considerable challenge.

While the Chinese government can do anything, it cannot do everything (Creemers, 2018). A significant challenge is an external rejection by citizens. While it is not always easy for Chinese citizens to oppose policies, there is no shortage of examples where central and local governments reconsidered or reversed decisions after protests. Creemers (2018) writes that more recently, the government's response to shutting down Tencent and Alibaba's social credit programs was due to increasing concerns about user privacy and underscores the need for citizens to be on board with state programs.

4 Combining State Social Scoring and Surveillance

This section delves into the integration of state surveillance and social scoring systems, with a particular focus on the potential harms of such a combination. First, it examines China's case to determine whether social credit scoring is facilitating state surveillance. Next, it considers the potential for similar systems to be implemented in other parts of the world. Finally, the section explores the harms associated with the combination of social scoring with state surveillance, particularly the impact on privacy, liberty, and fairness.

Surveillance is a key aspect of social control mechanisms (Hope, 2009). China's social credit system and its ongoing expansion of state surveillance represent a global movement for more efficient socio-economic control and enforcement of power (Loubere & Brehm, 2018). More states are using metrics and algorithms to govern society to improve perceived security (Ünver, 2018), public health (Lyon, 2019), and fairness within society (Werbach, 2022). Social credit systems are a new mode of governance that

combines law and governance and the public and private spheres (Backer, 2018). Backer argues that social credit systems will likely transform the structures and principles on which legal, governance, societal, and regulatory systems stand and through which they acquire legitimacy. Backer contends that social credit systems that enforce behaviour standards through data-driven analytics will shift the focus from public law and the constitution to the rule of analytics and algorithms. Backer writes that the extent to which one obeys the law will become as important as the mere act of obedience.

Social credit systems can be the ultimate commercialisation tool to exercise control (Lyon, 2019) because it provides incentives for maximising citizen value through politically and commercially aligned social behaviour (Loubere & Brehm, 2018). Rating systems could construct social norms by measuring adherence to rules and norms (Backer, 2018). Backer writes that governments have a long history of employing data as a simplifying mechanism to exercise and expand their authority. With technological advancements, extending states' authority is becoming much easier and cheaper. The border between political, social, and economic realms is becoming more blurred, creating the opportunity for abuse of power (Fuchs, 2019). Loubere & Brehm (2018) argue that it is not hard to envision a future where a digital social credit system sits at the core of a coercive state surveillance program.

4.1 China's case - is social credit scoring enabling state surveillance?

The CCP is increasingly legally codifying its control, such as controlling political expression online and placing restrictions on civil society (Drinhausen & Brussee, 2021). Werbach (2022) argues that, to date, the CSCSS is very basic and does not predict future behaviour nor identify hidden patterns. Drinhausen & Brussee write that the CSCSS primarily focuses on credit history and law enforcement, and there is no officially documented focus on conducting political surveillance of individual behaviour. However, the use of the CSCSS on political targets (Creemers, 2018) and the repressive COVID-19 pandemic control measures are examples of the use of the CSCSS as a repressive economic outlet for state surveillance (Drinhausen & Brussee, 2021). These 'non-credit' examples have come with widespread criticism. Drinhausen & Brussee contend that the CCP has much more concerning surveillance projects, such as Golden Shield, Skynet, Safe Cities, Police Clouds, and Project Sharp Eyes. The Integrated Joint-Operations Platform in Xinjiang is a very concerning mass surveillance program, as it has subjected over 13 million Uyghurs and Turkic Muslims to human rights violations (BBC News, 2022).

However, the CSCSS is potentially a core enabling program for the CCP's surveillance ambitions (Creemers, 2018). Hoffman (2019) writes that the CCP believes in social engineering - that individuals can be transformed and moulded- and that automated, data-based systems are the key to social control. The CCP is a repressive and authoritarian regime. Its history underscores its willingness to oppress citizens to stay in power - including concerns about human rights violations, abuse of state power, and free speech restrictions (Werbach, 2022). Creemers (2018) writes that state-owned media has called for more data-driven systems to inform policy-making, improve governance and inform economic and social trends. Werbach (2022) writes that most Chinese citizens explicitly endorse the system and are optimistic about the CSCSS as a legal enforcement tool. Further, the CSCSS is the most advanced state social scoring system to date. Its scope has expanded over time, recently seen in its use to economically harm citizens who did not comply with COVID-19 pandemic preventive measures (Brussee, 2023).

With a population of over 1.4 billion, over 800 million internet users, one of highest usages of CCTV cameras worldwide, and the tracking of internet and social media activity, it is not hard to see why the CSCSS is the most advanced state-led program worldwide (Werbach, 2022). Werbach contends that the CSCSS encompasses learnings from many pilot programs and highlights China's potential to be at the forefront of social scoring-enabled state surveillance. The issues and limitations identified in the previous chapter with the CSCSS might hamper further expansion. However, they may also be uniquely Chinese issues, specifically the localised implementation of laws and poor constitutional legislation.

4.2 Rest of world case to use social scoring systems to enable state surveillance

Social scoring systems represent the intersection of three global trends: the migration from human to digital decision-making, the shift from top-down regulation toward more sophisticated conceptions of governance, and the overwhelming belief in the power of big data and analytics to address virtually any problem (Werbach, 2022). Werbach argues that even if China's social credit experience turns out to be corrupt or repressive, key elements of the system's design may still be adopted elsewhere. Data-driven feedback incentives to shape behaviour are not unique to China (Loubere & Brehm, 2018). Algorithmic governance is growing even in liberal democracies with constitutional protections against unjust

impositions of state power (Jarman, 2021). Loubere & Brehm contend that social rating systems like the proposed social credit system will inevitably sit at the centre of surveillance regimes. They argue that social rating systems will provide the basis for how individuals and organisations are monitored and assessed and what they can (and cannot do) within society.

Werbach (2022) writes that a SSS in America would rest on different foundations compared to China. Werbach writes that the moral aspect of the CSCSS is unfamiliar to the West as, generally, systems are self-serving and meet material needs. Werbach argues that a SSS might exacerbate inequality and harm the most vulnerable in society. Creemers (2018) suggests that a Western implementation of a SSS will be more overt than the CSCSS. Western social control techniques, such as gamification or nudging, are essentially unnoticeable. Nudging exploits unconscious decision-making and inherent biases to steer individual behaviour. Creemers writes that the CSCSS, on the other hand, does not hide its paternalism under a bushel: it is part of an openly declared and widely propagated effort to instil civic virtue and to raise individuals' consciousness about their actions.

Unlike the CSCSS, which appears to exclude the private sector (Drinhausen & Brussee, 2021), private companies will likely play a prominent role in SSS in the West as entrepreneurs set their eyes on the available commercial opportunities (Werbach, 2022). A SSS in the West will likely focus less on the 'credit' aspect and more on the social incentive aspect because financial credit systems are advanced and established.

Some limitations identified in the CSCSS might also affect the implementation of similar programs in the West, such as issues with fragmentation and fairness (Creemers, 2018). A vital difference is that the West has well-established courts, constitutional rights, and privacy protection laws (Ünver, 2018). Ünver writes that perhaps the biggest hurdle will be public approval of an overt system, as dissent for any system appearing to encroach on privacy and freedom will be significant. States will find it challenging to implement a policy largely rejected by the citizenry.

4.3 Harms of social scoring enabled state surveillance

While social scoring may benefit society (Monahan, 2011), acceptance should not come without recognising the harm to individuals and society (Sætra, 2019). Werbach (2022) argues that implementing a

SSS, even remotely similar to the CSCSS, is deeply problematic for society due to various harms and exploitation risks. Some of the harms include erosion of individual privacy (Königs, 2022) and liberty (Sætra, 2019), a power distortion between the watcher and watched (Richards, 2013), repressive and discriminatory systems (Lyon, 2019), and the inability to live a normal life without participation in the system (Loubere & Brehm, 2018). Further, Sætra (2019) argues that the mere existence of individual data is a threat to society because of the risk of data leaks, hostile hacking attempts, the sale of data, change of ownership of companies, change of government, or simply a change in the intentions and plans of the actors that were once trusted.

4.3.1 Coerced Participation

Social credit systems establish an explicit and tangible link between social behaviour and economic benefits (Loubere & Brehm, 2018). As seen in the CSCSS and many private scoring systems, financial incentives such as discounts or fines underpin the rewards and punishments incentive. Loubere & Brehm write that social credit systems create new incentives that align the interests of citizens and organisations with those of the government. Loubere & Brehm argue that in this financial system, social action becomes increasingly entrenched within the economic realm, and individual behaviour is shaped increasingly by financial motives. Thus, integration into the socio-economic system is a necessity rather than a choice in a society dominated by social credit.

Further, for social credit systems to help improve untrustworthiness in society, everyone needs to be assessed equally; hence, the system requires the inclusion of all individuals (Loubere & Brehm, 2018). Loubere & Brehm write that without an information-driven social credit score, the burden of proving one's trustworthiness falls to the individual, as they will probably have the worst social score without any information. Citizens will find themselves increasingly nudged (if not enforced by regulation) to participate in these systems to lead normal lives and benefit from them (Werbach, 2022). This forced participation creates a paradox because the global financial inclusion project inadvertently results in socio-economic exclusion (Loubere & Brehm, 2018). Sætra (2019) argues that alternative choices should exist for there to be true freedom, and Feldstein (2020) suggests that citizens are running out of alternatives in modern society.

4.3.2 Privacy and Liberty

Much criticism for state surveillance and social scoring revolves around privacy concerns and Ünver (2018) argues that citizens have lost the war on privacy. Königs (2022) argues that there are three sources of concern where surveillance and social scoring systems diminish citizens' privacy: collecting citizens' data, accessing their data, and using the collected data for objectionable purposes. Königs (2022) argues that only the last two points are compelling concerns for privacy. However, Richards (2013) asserts that the mere collection of others' data undermines individual privacy because of the networked nature of Big Data. Richards writes that AI can derive information and characteristics about individuals by using the data of other similar individuals. Hence, it is possible to draw inferences from individuals whose information is limited by merely collecting others' information. Sætra (2019) argues that it is for the above reason that privacy is a public good and that it is the state's responsibility to prevent situations that force individuals to abandon their privacy to live normal lives.

Intellectual surveillance - the surveillance of what people are thinking, reading, and communicating with others is becoming more widespread (Richards, 2013). Intellectual surveillance includes tracking public sentiment through social media monitoring, surveilling protests, and monitoring journalists and government critics (Ünver, 2018). Chinese apps, such as WeChat, have built-in censorship and surveillance components, preventing the dissemination of politically sensitive material (Wong, 2020). Richards (2013) argues that intellectual surveillance is dangerous to society because it can cause people not to experiment with new, controversial, or deviant ideas or to make up their minds about political and social issues. Richards argues that free minds are the foundation of a free society. Kampmark (2014) writes about global petition arguing that "a person under surveillance is no longer free; a society under surveillance is no longer a democracy". Richards argues that surveilling intellectual activities that generate ideas and form individual beliefs can harm intellectual diversity and individuality.

4.3.3 Discrimination and Fairness

Technological systems based on big data and analytics are never simply neutral tools (Werbach, 2022). According to Werbach, they embed normative judgments and latent biases of their creators. The bias is especially true for systems initiated by governmental authorities that use automated decision-making.

While surveillance technology may seem inherently objective, machine learning models can exhibit biases and discriminate against marginalised groups (Lyon, 2019).

In 2019, a landmark study conducted by the Institute of Standards and Technology uncovered bias and discrimination within machine learning models. The study revealed higher misidentification rates for African American or Asian individuals compared to White males by up to 100 times (Wong, 2020). Wong express particular concern about the use of FRT in identifying, arresting, and detaining criminals due to the high misidentification rate of marginalised groups. Furthermore, the ongoing development of a sophisticated high-tech surveillance state in the Xinjiang Uyghur Autonomous Region anticipates a future where a SSS sits at the core of a coercive security apparatus inherently biased against specific segments of society (Kostka et al., 2023). Loubere & Brehm (2018) argue that SSS will lead to a dramatically inequitable society.

One significant concern regarding the CSCSS and similar systems is their potential lack of consistent rules (Werbach, 2022). Algorithms present a problem because their decisions may not be explainable or interpretable in the same way as human decisions (Loubere & Brehm, 2018). Werbach writes that algorithmic decisions are based on hidden patterns of correlations with no direct analogue to explanations humans can understand. Even if a consistent algorithmic rule is applied, many argue that rules and laws should be slightly flexible, allowing for the complexity of many situations. It is conceivable that algorithms would not have all the data available to make empathic and not seemingly arbitrary decisions (Fuchs, 2019). Edward Snowden asserts in his autobiography - "a world of total automated enforcement – of, say, all pet-ownership laws, or all zoning laws regulating home businesses – would be intolerable" (Snowden, 2019). Snowden argues that extreme justice can turn out to be extreme injustice. Königs (2022) affirms Snowden's assertion and argues that citizens do not desire consistent and thorough application of the law and that consistency is harmful.

4.3.4 Information is Power

Surveillance distorts the power relationships between the watcher and the watched as it grants the watcher greater power to influence or direct the subject of surveillance (Richards, 2013). Richards argues that this disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed

for wrongdoing unrelated to the purpose of the surveillance. Even in democratic societies, the threat of blackmail through surveillance is real. For example, Wong (2020) write that the two-year-long surveillance of civil rights leader Martin Luther King yielded evidence of his marital infidelity and was used to try and blackmail him. Richards (2013) argues that surveillance enhances the watcher's ability to persuade, which is a subtler but potentially more effective exercise of this power differential compared to blackmail. It is especially concerning when states use social scoring systems to persuade individuals through commercial means.

Richards (2013) argues that many surveillance programs' secretive nature and the outdated regulations and frameworks exacerbate the power imbalance. Richards points out that many existing frameworks are outdated because they assume targeted data collection rather than systematic data collection (Rubinstein et al., 2017). Further, many policies are geographically focused, and Rubinstein et al. argue that lower policy standards apply across borders. The secrecy surrounding state surveillance makes it difficult to have a public debate about the extent of these programs. Richards (2013) discusses numerous court cases against the American state and its surveillance agencies. In many cases that Richards references, the defence could not prove that the government was surveilling a specific individual and, therefore, could not definitively establish a First Amendment violation. The secrecy of state surveillance programs and the difficulty in obtaining more information about them due to the state secrets doctrine were the primary reasons for the unsuccessful cases.

Private companies play an increasingly powerful and vital role in state surveillance as surveillance becomes increasingly commercialised through state and private company partnerships (Fuchs, 2019). The datasets of most significant interest to intelligence agencies are no longer government-owned or produced; they are created and owned by private companies (Zuboff, 2019). In addition to demanding systematic access to the data, states require private-sector entities to retain data on demand (Rubinstein et al., 2017). Rubinstein et al. raise concerns about transparency, accountability, and proportionality when states access data held by private entities. For example, law enforcement agencies partner with Amazon Ring to facilitate the voluntary handover of Ring video footage without a warrant (Turner Lee & Chin-Rothmann, 2022). Zuboff (2019) argues that companies focus on profit maximisation at the cost of individual privacy and that this new commercialised form of surveillance is particularly concerning. Wong (2020) argues that companies do not take into account the impact on people who use or are

affected by their surveillance products because there is no market incentive to do so. Further, private companies are more overt with what they do with individual data, often hiding behind proprietary closed-source code, non-disclosure agreements, and vertical organisation to obfuscate their practices (Sætra, 2019).

Königs (2022) presents two reasons for concern regarding the expansion of surveillance capacities in established democracies. Firstly, Königs argues that established democracies may undergo decay, a view supported by Feldstein (2022), who suggest that this decay is already underway. Königs writes that democratically legitimate surveillance purposes today could be used for poorly legitimated purposes in the future. Sætra (2019) supports this view and posits that in the future, information may find new and unconventional applications distinct from its original intent Secondly, Königs argues that the democratic procedures within established democracies fail to conform to the requirements formulated by mainstream theories of democracy. Königs maintains that state institutions in established liberal democracies are already flawed, and the process for debating new policies is inadequate.

5 Conclusion

State surveillance has expanded its scope to the routine and systematic collection of personal data (Königs, 2022). Rapid expansions in state surveillance have occurred due to threats to national security from extremist terrorist attacks, significant advancements in data capture and surveillance technology, and regulations that are lagging behind these changes (Steinfeld, 2017). Machines have taken over domains that historically seemed to require human judgment, like facial recognition and city policing (Pozen, 2016). National identification programs and machine learning techniques enable states to gather and infer more individual information than ever before, using this information to predict future behaviour (Turner Lee & Chin-Rothmann, 2022). The COVID-19 pandemic caused a boom in surveillance technology sales (Eck & Hatz, 2020) as states disregarded privacy concerns and implemented pervasive control measures to suppress the outbreak (Miyamoto, 2020). A big concern arises from the potential persistence of pandemic surveillance and control measures beyond the pandemic (Kampmark, 2020). Governments worldwide have partnered with private companies, such

as Clearview AI and Landasoft (Feldstein, 2022), and have integrated surveillance into the commercial sphere (Lyon, 2019).

Surveillance is a key aspect of social control mechanisms (Hope, 2009). Social scoring systems represent the intersection of three global trends: the migration from human to digital decision-making, the shift from top-down regulation toward more sophisticated conceptions of governance, and the overwhelming belief in the power of big data and analytics to address virtually any problem (Werbach, 2022). The border between political, social, and economic realms is becoming more blurred, creating the opportunity for abuse of power (Fuchs, 2019). Loubere & Brehm (2018) reason that it is not hard to envision a future where a digital social credit system sits at the core of a coercive state surveillance program. Social surveillance systems will be the basis for monitoring and assessing individuals and organisations and determining what they can (and cannot) do within society. The CSCSS represents a relatively basic social system with various limitations, including fragmentation, arbitrary implementation, poor digitisation, and low take up rates (Drinhausen & Brussee, 2021). A social surveillance and scoring system in the West will most likely involve more private company support and be more overt (Wong, 2020). However, it could face similar challenges as the CSCSS, especially meagre public approval rates (Creemers, 2018).

As a society, we are thus of two minds about surveillance (Richards, 2013). On the one hand, states have legitimate reasons to undertake surveillance that is not rooted in a desire to enforce political repression and limit individual freedoms (Feldstein, 2020). States have found themselves in predicaments as many citizens view them as responsible for domestic security, public health, and ensuring trustworthy markets (Ziller & Helbling, 2021). On the other hand, abuse of power and discrimination are significant risks associated with social surveillance (Loubere & Brehm, 2018). Social surveillance encroaches on privacy (Königs, 2022) and liberty (Sætra, 2019), creates a power imbalance (Richards, 2013) and results in the individuals' inability to live a normal life without participation in the system (Loubere & Brehm, 2018). A big concern is that corporate and state surveillance is a crucial feature of living in today's modernised world (Ziller & Helbling, 2021). Surveillance is entrenched in everyday life, resulting in a surveillance society with questionable areas of life still private (Westerlund et al., 2021).

As democracies decline, surveillance's harmful impacts are further exacerbated (Drinhausen & Brussee, 2021). Troubling surveillance activity occurs in all political contexts (Feldstein, 2020), and citizens' willingness to accept these measures comes into question. Individuals willingly surrender some of their liberties due to threats of terrorism and for the greater public good, even if it may seem irrational (Wang, 2021). Systematic surveillance programs have outpaced regulatory efforts (Rubinstein et al., 2017).

The choice should not be between privacy or security, public health or pandemics, financial inclusion or exclusion, or social inclusion or exclusion, but rather how individual liberty and rights could be protected while simultaneously improving the lives of all. States must balance conflicting parameters (Pozen, 2016) and ultimately leave citizens with viable alternative choices. As social surveillance technology evolves, researchers and advocates must document how states and companies manage new uses of surveillance technology and social scoring systems. Social surveillance programs should not operate secretly, and citizen consent and buy-in should be prioritised (Ünver, 2018).

The findings of this literature review are significant as they reveal the complex interplay between technological advancements, state surveillance, and individual freedoms. State surveillance and social scoring systems not only impact individual privacy and freedoms but also impact broader societal dynamics. A robust, global debate is needed to develop appropriate frameworks that guide the use of new surveillance technologies to strike the correct balance between citizens' rights and law enforcement needs (Wong, 2020). The urgency of developing appropriate regulatory frameworks and raising public awareness cannot be overstated. By understanding the implications of these surveillance systems, stakeholders can work towards creating a balanced approach that safeguards privacy while addressing security and governance needs.

5.1 Limitations and Future Research

Using social scoring as an enabler for state surveillance is a relatively nascent field, necessitating further exploration of how these systems differ across various contexts. As personal privacy regulations evolve to keep pace with technological advancements, it is crucial for researchers to study the effectiveness of these new regulations. Additionally, future research should focus on public perception of surveillance and the ethical implications of social scoring systems. By investigating these areas,

researchers can develop comprehensive strategies that balance the benefits of surveillance with the protection of individual rights.

Bibliography

Backer, L. C. (2018). Data Driven Governance: Building Data Driven Accountability Based Regulatory Systems in the West and Social Credit Regimes in China. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3209997

BBC News. (2022). Who Are the Uyghurs and Why Is China Being Accused of Genocide?. *BBC*.

Boersma, K., Van Brakel, R., Fonio, C., & Wagenaar, P. (2014). *Histories of State Surveillance in Europe and Beyond* (0th ed.). Routledge. https://doi.org/10.4324/9780203366134

Boudreaux, B. (2020). *STRENGTHENING PRIVACY PROTECTIONS: In COVID-19 Mobile Phone-Enhanced Surveillance Programs*.

Breckenridge, K. D., Szreter, S., & Academy, B. (2012). *Registration and Recognition: Documenting the Person in World History* (Issue 182). Published for the British Academy by Oxford University Press.

Brussee, V. (2023). *Social Credit: The Warring States of China's Emerging Data Empire*. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-2189-8

Caplan, J., & Torpey, J. (2001). *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press.

Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3175792

Drinhausen, K., & Brussee, V. (2021). *China's Social Credit System in 2021: From Fragmentation towards Integration*.

Eck, K., & Hatz, S. (2020). State Surveillance and the COVID-19 Crisis. *Journal of Human Rights*, *19*(5), 603–612. https://doi.org/10.1080/14754835.2020.1816163

Feldstein, S. (2020). *State Surveillance and Implications for Children*.

Feldstein, S. (2022). *The Global Struggle Over AI Surveillance: Emerging Trends and Democratic Responses*.

Foreign Policy. (2013). *The Surveillance State and Its Discontents*. *203*, 64–74.

Fuchs, C. (2019). Karl Marx in the Age of Big Data Capitalism. In C. Fuchs & D. Chandler (Eds.), *Digital Objects, Digital Subjects: Digital Objects, Digital Subjects* (pp. 53–72). University of Westminster Press.

Gershgorn, D. (2020, May). *We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World.*

Haggerty, K. D., & Samatas, M. (2010). *Surveillance and Democracy* (0th ed.). Routledge-Cavendish. https://doi.org/10.4324/9780203852156

Higgs, E. (2004). *The Information State in England The Central Collection of Information on Citizens Since 1500*. Macmillan Education UK, 2004.

Hoffman, S. (2019). *Managing the State: Social Credit, Surveillance, and the Chinese Communist Party's Plan for China* (pp. 48–54).

Hope, A. (2009). CCTV, School Surveillance and Social Control. *British Educational Research Journal*, *35*(6), 891–907.

Horsley, J. (2028, November). *China's Orwellian Social Credit Score Isn't Real.*

Ioannou, A., & Tussyadiah, I. (2021). Privacy and Surveillance Attitudes during Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours. *Technology in Society*, *67*, 101774. https://doi.org/10.1016/j.techsoc.2021.101774

Jarman, H. (2021). Governance, surveillance, coercion, and social policy. In *Coronavirus Politics The Comparative Politics and Policy of COVID-19* (pp. 51–64).

Jarvis, L. (2022). Critical Terrorism Studies and the Far-Right: Beyond Problems and Solutions?. *Critical Studies on Terrorism*, *15*(1), 13–37. https://doi.org/10.1080/17539153.2021.2017484

Kampmark, B. (2014). Restraining the Surveillance State: A Global Right to Privacy. *Journal of Global Faultlines*, *2*(1). https://doi.org/10.13169/jglobfaul.2.1.0001

Kampmark, B. (2020). The Pandemic Surveillance State: An Enduring Legacy of COVID-19. *Journal of Global Faultlines*, *7*(1). https://doi.org/10.13169/jglobfaul.7.1.0059

Kim, J., & Kwan, M.-P. (2021). An Examination of People's Privacy Concerns, Perceptions of Social Benefits, and Acceptance of COVID-19 Mitigation Measures That Harness Location Information: A Comparative Study of the U.S. and South Korea. *ISPRS International Journal of Geo-Information*, *10*(1), 25. https://doi.org/10.3390/ijgi10010025

Knight, A. (2023). Basket Case: Reform and China's Social Credit Law. *China Law and Society Review*, *6*(2), 181–210. https://doi.org/10.1163/25427466-06020003

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under Big Brother's Watchful Eye: Cross-country Attitudes toward Facial Recognition Technology. *Government Information Quarterly*, *40*(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. *Philosophy & Technology*, *35*(1), 8. https://doi.org/10.1007/s13347-022-00503-9

Lauer, J. (2012). Surveillance History and the History of New Media: An Evidential Paradigm. *New Media & Society*, *14*(4), 566–582. https://doi.org/10.1177/1461444811420986

Li, H., & Kostka, G. (2022). Accepting but Not Engaging with It: Digital Participation in Local Government-Run Social Credit Systems in China. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4066462

Liu, C. (2023). A Tale of Two Social Credit Systems: The Succeeded and Failed Adoption of Machine Learning in Sociotechnical Infrastructures. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4454705

Loubere, N., & Brehm, S. (2018). The Global Age of Algorithm: Social Credit and the Financialisation of Governance in China. *Made in China Journal*, *3*(1). https://doi.org/10.22459/MIC.03.01.2018.07

Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are Counter-Terrorism Strategies Effective? The Results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research. *Journal of Experimental Criminology*, *2*(4), 489–516. https://doi.org/10.1007/s11292-006-9020-y

Lyon, D. (2019). *State and Surveillance* (pp. 21–25).

Miyamoto, I. (2020). *Mass Surveillance and Individual Privacy*.

Monahan, T. (2011). Surveillance as Cultural Practice. *The Sociological Quarterly*, *52*(4), 495–508.

Nabity-Grover, T., Cheung, C. M., & Thatcher, J. B. (2020). Inside out and Outside in: How the COVID-19 Pandemic Affects Self-Disclosure on Social Media. *International Journal of Information Management*, *55*, 102188. https://doi.org/10.1016/j.ijinfomgt.2020.102188

Nam, T. (2019). What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates. *The Social Science Journal*, *56*(4), 530–544. https://doi.org/10.1016/j.soscij.2018.10.001

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119.

Piotrowicz, C. (2019). Predictive Policing:. *European Law Enforcement Research Bulletin*, *4SCE*, 107–111.

Pozen, D. E. (2016). Privacy-Privacy Tradeoffs. *The University of Chicago Law Review*, *83*(1), 221–247.

Research Markets. (2022). Global Surveillance Camera Market to 2027 with Chinese Companies Such as Hikvision and Dahua Dominating the Market. *Globenewswire News Room*.

Richards, N. M. (2013). THE DANGERS OF SURVEILLANCE. *HARVARD LAW REVIEW*, *126*.

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2017). Systematic Government Access to Private-Sector Data: A Comparative Analysis. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Bulk Collection* (1st ed., pp. 5–46). Oxford University PressNew York. https://doi.org/10.1093/oso/9780190685515.003.0001

Sankar, P. (1992). *State Power and Record-keeping: The History of Individualized Surveillance in the United States, 1790-1935*. University of Pennsylvania.

Schroeder, R. (2022). Aadhaar and the Social Credit System: Personal Data Governance in India and China. *International Journal of Communication*, *16*(0), 17.

Snowden, E. (2019). *Permanent Record*. Metropolitan Books.

Steinfeld, N. (2017). Track Me, Track Me Not: Support and Consent to State and Private Sector Surveillance. *Telematics and Informatics*, *34*(8), 1663–1672. https://doi.org/10.1016/j.tele.2017.07.012

Sætra, H. S. (2019). Freedom under the Gaze of Big Brother: Preparing the Grounds for a Liberal Defence of Privacy in the Era of Big Data. *Technology in Society*, *58*, 101160. https://doi.org/10.1016/j.techsoc.2019.101160

TED. (2014, October). *Glenn Greenwald: Why Privacy Matters*.

Turner Lee, N., & Chin-Rothmann, C. (2022). *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*.

Vincent, J. (2021, April). *FBI Used Facial Recognition to Identify a Capitol Rioter from His Girlfriend's Instagram Posts*.

Wang, J. (2021, January). *An In-depth Review of Privacy Concerns Raised by the COVID-19 Pandemic* (Issue arXiv:2101.10868). arXiv. https://doi.org/10.48550/arXiv.2101.10868

Werbach, K. (2022, September). *Orwell That Ends Well: Social Credit as Regulation for the Algorithmic Age* (Issue 3589804). https://doi.org/10.2139/ssrn.3589804

Westerlund, M., Isabelle, D. A., & Leminen, S. (2021). Perspectives from Higher Education: Applied Sciences University Teachers on the Digitalization of the Bioeconomy : The Acceptance of Digital Surveillance in an Age of Big Data. *Technology Innovation Management Review*, *11*(3), 32–44. https://doi.org/10.22215/timreview/1427

Wired. (2019). *The complicated truth about China"s social credit system*. 64–74.

Wong, D., Steven Feldstein. (2020, August). *New Technologies, New Problems – Troubling Surveillance Trends in America*.

Wong, T., & BBC Chinese. (2022). Henan - China Covid app restricts residents after banking protests. *BBC News*.

Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Deep Ganguli, B., Grosz, T. L., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R. (2021). *Artificial Intelligence Index Report 2021*.

Ziller, C., & Helbling, M. (2021). Public Support for State Surveillance. *European Journal of Political Research*, *60*(4), 994–1006. https://doi.org/10.1111/1475-6765.12424

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile books.

Ünver, H. A. (2018). *Politics of Digital Surveillance, National Security and Privacy*.