ARETE

Politik Felsefe Dergisi
Journal of Political Philosophy

The Panopticon Revisited: Surveillance, Discipline, and the Modern Political Order

Birol AKDUMAN*

Abstract

This study offers a comprehensive investigation into the expanding influence of surveillance in today's societies. Drawing on the pioneering theories of Jeremy Bentham's Panopticon and Michel Foucault's reflections on its far-reaching societal implications, the study provides an in-depth analysis of the dynamic shifts in power, discipline, and conformity within the context of our increasingly interconnected world. It critically examines how advancements in digital technologies, such as artificial intelligence, Internet of Things, and sophisticated data mining tools, have profoundly amplified the reach of the Panopticon, enabling a level of monitoring and control previously inconceivable. This narrative dives deep into the intricate power relationships

---

* **Dr.** ǀ **Phd**
Dokuz Eylül Üniversitesiǀ, **Dokuz Eylül University.**
birol_akduman@outlook.com
Orcid Id: 0000-0003-4049-0449

and regulatory dynamics that emerge from this hyper-surveillance society, illustrating how these technological mechanisms subtly yet powerfully shape human behaviors and societal norms. Notably, the study underscores the emergence of a culture of self-discipline and self-surveillance in our digital age. It illuminates how individuals, in the course of their daily interactions on social media and other digital platforms, often voluntarily divulge personal information, inadvertently contributing to the expansion of this modern Panopticon. Moreover, this discourse delves into the potential future direction of panopticism, taking into account the ramifications of emerging technologies such as facial recognition and biometric surveillance, predictive policing, and algorithmic decision-making. The potential consequences of these advancements on personal liberties, democratic procedures, and wider societal patterns are critically examined. The study offers a detailed and multifaceted evaluation of the swiftly changing terrains of authority and supervision in the digital epoch. By elucidating the profound effects of an omnipresent, technologically-enhanced panoptical oversight, the research adds significant insights to an essential academic debate on privacy, surveillance, and the future trajectory of our increasingly digitized societies.

Keywords: Panopticon, Surveillance, Discipline, Modern Political Order, Foucault.

Panoptikon'a Yeniden Bakış: Gözetim, Disiplin ve Modern Politik Düzen

Özet

Bu çalışma, "Panoptikon'a Yeniden Bakış: Gözetim, Disiplin ve Modern Politik Düzen" başlığı altında, günümüz toplumlarında gözetimin genişleyen etkisine kapsamlı bir araştırma sunmaktadır. Jeremy Bentham'ın Panoptikon'u ve Michel Foucault'nun bu konu üzerinde toplumsal etkileri olan düşüncelerini temel alarak, giderek daha girift bir yapıya evirilen dünyamızın güç, disiplin ve uyum üzerindeki dinamik değişikliklere derinlemesine bir analiz gerçekleştirilmektedir. Çalışma, yapay zeka, nesnelerin interneti ve sofistike veri madenciliği araçları gibi dijital teknolojilerdeki ilerlemelerin, daha önce tasavvur edilemeyen bir denetim ve kontrol düzeyine olanak sağlayarak Panoptikon'un erişimini ne denli artırdığını eleştirel bir şekilde inceler. Bu meta-anlatı, bu hiper-gözetim toplumundan ortaya çıkan karmaşık güç ilişkileri ve düzenleyici dinamiklere derinlemesine dalarken bu teknolojik mekanizmaların insan davranışlarını ve toplumsal normları nasıl hassas fakat güçlü bir şekilde şekillendirdiğini gösterir. Özellikle, dijital çağımızda bir öz-disiplin ve öz-gözetim kültürünün ortaya çıkışı vurgulanmıştır. Günümüzde sosyal medyada ve diğer dijital platformlarda günlük etkileşimler sırasında bireylerin genellikle kişisel bilgileri gönüllü olarak açığa çıkardıkları ve bu modern Panoptikon'un genişlemesine bilmeden katkıda bulundukları aydınlatılmaktadır. Ayrıca, bu söylem, yüz tanıma ve biyometrik gözetleme, proaktif polislik ve algoritmik karar verme gibi gelişmekte olan teknolojilerin sonuçlarını dikkate alarak panoptizmin potansiyel geleceğine dair projeksiyonlar üretir. Bu ilerlemelerin kişisel özgürlükler, demokratik işlemler ve geniş toplumsal desenler üzerindeki olası sonuçları eleştirel bir şekilde incelenmektedir. Çalışma, dijital dönemde hızla değişen otorite ve denetim bölgelerinin ayrıntılı ve çok yönlü bir değerlendirmesini sunar. Her yerde bulunan, teknolojik olarak gelişmiş bir panoptik gözetlemenin derin etkilerini açığa çıkararak, araştırma, gizlilik, gözetleme ve giderek dijitalleşen toplumlarımızın gelecek yönü üzerine önemli bir akademik tartışmaya kritik iç görüler eklemler.

Anahtar Kelimeler: Panoptikon, Gözetim, Disiplin, Modern Siyasi Düzen, Foucault ve Gözetim.

Methodology

The methodology employed in this study is comprehensive, spanning a vast array of inter-disciplinary approaches. Grounded in the disciplines of political theory, philosophy, strategic studies, international affairs, history, and sociology, the methodologies adopted work in synergy to enhance our understanding of the intricacies of surveillance, discipline, and the prevailing political order.

The principal analytical instrument used is a meticulous examination and interpretation of both primary and secondary materials. The works of scholars like Michel Foucault and Jeremy Bentham serve as primary sources, and they are carefully scrutinized to extract their viewpoints on the Panopticon and the surveillance society. Meanwhile, secondary sources, including an assortment of scholarly articles and books, offer a variety of interpretations and insights, thereby enriching the research's depth.

To effectively weave these disciplines together, a thematic analysis is implemented. This involves identifying and analyzing patterns or "themes" within the data collected from the primary and secondary resources. The data is scrutinized and coded to identify themes that emerge, which are then reviewed and refined to formulate the arguments presented in this paper.

Additionally, a historical analysis is implemented to contextualize the evolution of surveillance mechanisms and the concept of discipline. This analysis investigates how these concepts have been informed by and evolved through socio-political changes over time.

In the final stages, this study deploys a comparative approach, scrutinizing varying viewpoints on the Panopticon and surveillance society from the previously mentioned disciplines. This approach enhances the analysis, providing a more layered comprehension of the topic at hand while drawing attention to the convergences and disparities among these viewpoints.

In essence, the methodology chosen for this study aspires to deliver an all-encompassing, multi-dimensional scrutiny of the Panopticon and the contemporary political order, enabling a thorough investigation of this intricate and pertinent subject.

Introduction

As a historical artifact and symbol, the Panopticon, formulated by Jeremy Bentham in the late 18th century, has firmly established itself as a dominant metaphor for modern surveillance (Bentham, 1995, p. 29). The Panopticon, originally a novel architectural design for prisons, has been employed by scholars across disciplines as an illustrative tool to capture surveillance's pervasive and intrusive nature in contemporary societies (Foucault, 1977, p. 195).

Beginning with Michel Foucault's "Discipline and Punish," the Panopticon has been reimagined as a metaphor for the nature of modern surveillance mechanisms, exerting a form of discipline in society that is both pervasive and invisible (Foucault, 1977, p. 201). The central watchtower, invisible inmates, and the power dynamics it creates, symbolize the state's ability to monitor individuals, instilling a sense of constant surveillance and thus, enforcing self-discipline (Foucault, 1977, p. 202).

The Panopticon's design has been interpreted as a metaphor for the workings of modern power and surveillance, enabling a few to control many (Zuboff, 2019, p. 65). Today, scholars like Shoshana Zuboff have extended this metaphor to digital surveillance, highlighting how tech firms constantly monitor users' online activities (Zuboff, 2019, p. 81). This digital Panopticon creates a new form of surveillance capitalism, where personal data is the new oil (Zuboff, 2019, p. 83).

Simultaneously, the Panopticon metaphor has been critiqued as oversimplifying the complexities of modern surveillance systems. David Lyon, for instance, points out the Panopticon's inability to account for the fragmented and decentralized nature of contemporary surveillance (Lyon, 2006, p. 41). Also, the metaphor fails to consider the agency of the surveilled, the negotiation of power, and resistance to surveillance (Haggerty, 2006, p. 28).

In the era of globalization, the Panopticon metaphor is being re-evaluated. With the spread of technological innovations like artificial intelligence and big data, surveillance has transcended national boundaries, becoming a tool for both state actors and private entities (Bauman & Lyon, 2013, p. 11). This leads to a discussion on whether the

Panopticon still holds relevance as a metaphor for surveillance in our increasingly interconnected world.

The Panopticon metaphor, while illuminating, is limited. It captures the essence of surveillance but misses the nuances of the modern surveillance order where power dynamics are more fluid and complex. As scholars, it is our task to continually reassess and refine our metaphors to better understand and illuminate the realities we confront.

Unraveling the Panopticon: Bentham's Architectural Marvel and Foucault's Interpretation

To comprehend the Panopticon's evolution and its multifaceted implications in the modern political order, it is vital to trace its roots back to its architect - Jeremy Bentham. As an English philosopher and social theorist of the 18th century, Bentham's vision of the Panopticon was an architectural marvel aimed at reforming the societal structure through enhanced surveillance (Semple, 1993, p.37).

In his seminal work, "Panopticon; or The Inspection-House" (1791), Bentham introduced the Panopticon as an "ideal architectural figure" for various establishments such as prisons, factories, workhouses, and hospitals (Bentham, 1791, p.45). This circular structure was designed with a central watchtower overseeing the enclosed cells arranged in a peripheral ring, where inmates could be observed without being aware of when exactly they were being watched.

Bentham conceptualized this design not merely as a physical structure but as a metaphor for power and control. The Panopticon's power lay in the "unverifiable" nature of its surveillance - the constant possibility of observation led to self-discipline among the inmates, a revolutionary concept in the disciplinary society (Foucault, 1977, p.201). In Bentham's perspective, the Panopticon was the embodiment of "the perfect exercise of power" that could render its holders "omnipresent and omniscient" (Bentham, 1791, p.45).

This mechanism of power, however, extends beyond Bentham's original intent of societal reform. The Panopticon has been critiqued as a tool for oppressive control. Bentham's brother, Samuel, for example, initially implemented the design in the mills of

the Industrial Revolution in Russia, and it was later utilized in the colonial contexts as a symbol of dominance (Zuboff, 2019, p.65).

The Panopticon's enduring influence signifies its transition from an architectural marvel to a pervasive metaphor in the modern political order. It represents a crucial shift in societal control mechanisms, from overt coercive methods to subtle, internalized surveillance systems, that have restructured power dynamics across multiple dimensions (Bauman & Lyon, 2013, p.25). This section explores this multifaceted transformation in detail, offering an in-depth understanding of the Panopticon's origins, its evolution, and its implications in today's surveillance society.

The panopticon concept, as postulated by Jeremy Bentham, gains a profound insight when viewed through the lens of Michel Foucault, a renowned 20th-century philosopher, and social theorist. Foucault, in his groundbreaking work "Discipline and Punish" (1977), interpreted the panopticon not merely as an architectural marvel but as a metaphor for power relations intrinsic to modern societies. His analysis of the panopticon serves as a critical commentary on the insidious nature of surveillance that perpetually haunts contemporary life.

Foucault's exploration of the panopticon was intricately woven into his broader discourse on 'disciplinary society.' As per Foucault (1977), modern societies exert control not through overt coercion or physical force but through subtle, omnipresent systems of discipline maintained through the constancy of surveillance. This system of power, according to him, is perfectly epitomized by Bentham's panopticon, where the mere potential of being observed is sufficient to modulate behavior (p.201).

Foucault (1977) proposed that the principles of the panopticon extend beyond the confines of prisons and infiltrate various societal institutions, such as schools, hospitals, and workplaces (p.205). The mantra of the panopticon, 'to see without being seen,' is echoed in these structures, subtly coercing individuals to adhere to societal norms and regulations under the continual scrutiny of an invisible observer. In effect, Foucault reinterpreted the panopticon from a physical edifice to a societal construct that shapes, controls, and disciplines behavior.

Underpinning Foucault's interpretation of the panopticon is the concept of discipline through the fear of constant visibility. The panopticon instills a consciousness of continual surveillance, even when actual observation is absent. This self-regulating mechanism, born out of the fear of being watched, Foucault argues, is far more effective than any tangible constraint. The true potency of the panopticon lies in its ability to 'induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power' (Foucault, 1977, p.201).

Foucault's conceptualization of the panopticon has been met with varying academic responses. Scholars such as Deleuze (1992) have argued that Foucault's panopticism becomes increasingly irrelevant in our 'post-panoptic' society, where digital surveillance and data collection are prevalent (p.5). However, others counterargue that the emergence of digital surveillance technologies, such as CCTVs, GPS tracking, and internet monitoring, reinforce and extend Foucault's vision of a panoptic society, rendering it more omnipresent and insidious than ever before.

In conclusion, Michel Foucault's interpretation of the panopticon as a metaphor for contemporary surveillance and social control offers a compelling critique of our societal power dynamics and control mechanisms. His analysis serves as a stark reminder of our place within this metaphorical panopticon, under the ceaseless gaze of an unseen observer, persistently modulating our behavior to align with perceived societal norms and expectations.

Foucault's interpretation of the panopticon symbolically represents the mechanisms of power and control embedded in contemporary society. He posits that the panopticon's design principle of visibility as a trap (1977, p.200) has been adopted by modern states as a tool to maintain discipline, order, and conformity. From schools to workplaces, hospitals to military barracks, Foucault contends that the 'panoptic' schema has been replicated and integrated into the fabric of our institutional structures. This schema becomes internalized within the individual, creating a self-regulatory society where discipline becomes an automated, decentralized process (Foucault, 1977, p.202).

Foucault's understanding of the panopticon presents a unique insight into the nature of modern surveillance. Today's surveillance systems, much like the panopticon, are often invisible and unverifiable, yet their omnipresence is felt. This sentiment is increasingly

palpable in the digital age, where our every move, click, and interaction can be tracked, recorded, and analyzed. This constant digital surveillance, according to scholars like Lyon (2001), amplifies the panoptic effect, creating what they term a 'surveillance society' (p.2).

In Foucault's analysis, the power of the panopticon lies not in the act of surveillance itself, but rather in the psychological impact it exerts on the individual. The panopticon induces a state of conscious and permanent visibility that assures the automatic functioning of power (Foucault, 1977, p.201). The mere possibility of being watched compels individuals to adjust their behavior, reinforcing their adherence to societal norms and rules. Foucault's interpretation therefore illuminates how surveillance operates not only as a system of control but also as a mechanism for manufacturing consent.

While Foucault's examination is noteworthy, it has faced its share of criticisms. Notably, academics such as Galloway (2012) contend that the Panopticon's central premise might be overly reductive when used to elucidate the intricate nature of contemporary digital surveillance (p.140). The Panopticon posits a singular, centralized monitoring entity, but the reality of digital surveillance encompasses numerous observers, concurrently active across disparate platforms. This decentralized surveillance, or 'protocol' as Galloway (2012) categorizes it, disputes the conventional Panopticon's paradigm (p.142).

In spite of these criticisms, the implications of Foucault's panopticon interpretation as an apparatus of observation and societal regulation remain pertinent. His reflections deliver a conceptual scaffold to comprehend the intrinsic power mechanisms in present-day monitoring systems. Regardless of whether in tangible environments or digital domains, the panoptic philosophy of 'observing without being observed' is omnipresent in our lives, steering our conduct and affecting our social engagements.

Technological Reinforcement of the Panopticon: Surveillance in the 21st Century

In our journey through the evolution of surveillance, we encounter a significant leap with the advent of Closed-Circuit Television (CCTV) and facial recognition technology. These modern iterations of the Panopticon concept have proliferated globally, becoming ubiquitous fixtures in urban landscapes (Norris & Armstrong, 1999, p. 56).

The CCTV system, a significant development in surveillance technology, offers the potential for continuous and omnipresent observation. The UK, often cited as the world leader in CCTV usage, has approximately one camera for every 11 people, illustrating the enormity of its surveillance capacity (McCahill & Norris, 2002, p. 85). This breadth of surveillance has been justified by governments and security agencies as a necessary tool in maintaining public safety and deterring crime (Goold, 2004, p. 101). However, critics argue that its effectiveness remains questionable and that it predominantly serves as a tool of social control, echoing Foucault's analysis of the Panopticon (Gill & Spriggs, 2005, p. 33).

This social control extends beyond CCTV into the realm of facial recognition technology. The capability of facial recognition systems to identify individuals from images or video sources has further amplified the Panopticon's metaphorical gaze (Jenkins & Carle, 2011, p. 209). By transforming faces into data points that can be analyzed, categorized, and stored, it creates a digital identity that allows for tracking across multiple platforms and locations (Introna & Wood, 2004, p. 177).

China, for instance, uses this technology extensively, particularly in the Xinjiang region, where it has been implicated in the surveillance and control of the Uighur population, raising significant human rights concerns (Ramzy & Buckley, 2019, para. 5). However, this technology isn't confined to authoritarian regimes; democratic countries, such as the United States and the UK, also deploy facial recognition systems extensively, often under the banner of counter-terrorism and crime prevention (Fussey & Murray, 2019, p. 90).

While these technologies have undoubtedly enhanced surveillance capabilities, they have also intensified the debates around privacy, civil liberties, and the power dynamics inherent in surveillance. Therefore, the Panopticon metaphor remains salient in framing our understanding of the dynamics of power and control in a surveillance society. However, this metaphor's application in an era of digital surveillance does require reinterpretation, which will be explored further in the next section.

In the current digital era, data functions as an essential tool for surveillance, rendering privacy an increasingly elusive concept. The pervasiveness of data collection makes it a direct successor of the Panopticon, where the unseen observer is now the

myriad of interconnected devices and applications that collect, analyze, and store personal data (Zuboff, 2019, p.45).

From online purchases and social media interactions to smart home devices and wearable technology, personal data is constantly being harvested, often without the user's explicit consent or knowledge. The ubiquitous nature of this data collection process represents a form of surveillance that echoes the principles of the Panopticon. These vast amounts of data, often referred to as 'big data', are analyzed using sophisticated algorithms and artificial intelligence (AI) to gain insights into individual behaviors and preferences (Tene & Polonetsky, 2013, p.239).

This continuous, pervasive surveillance, as Lyon (2001, p.2) suggests, has significantly shifted the power dynamics between individuals and entities that collect and control data. Just as prisoners in the Panopticon were subject to the gaze of an unseen guard, individuals in the digital age are subject to the gaze of unseen data collectors and analysts. However, the power in this modern Panopticon is not only based on the possibility of being observed, but also on the potential misuse of the information collected.

The implications of this shift are multifaceted and profound. For instance, Solove (2007, p.748) points out that this unrelenting data collection and the subsequent potential for privacy invasion have generated a chilling effect on individual behaviors. People may self-censor or modify their behavior due to the awareness that their actions are being tracked, stored, and potentially scrutinized.

Additionally, corporations such as Facebook and Google, holding a significant portion of individual data, can alter user activity to align with their corporate agendas. This issue was exposed in the controversy surrounding Cambridge Analytica, a political consultancy that unethically accessed the data of numerous Facebook users to sway voting patterns (Cadwalladr & Graham-Harrison, 2018). This event serves as a stark warning of the possible misapplication of data and the consequent danger to democratic procedures.

Moreover, state surveillance initiatives, like the PRISM program of the U.S. National Security Agency, which amasses and scrutinizes data on an unparalleled scale,

instigate grave apprehensions about citizens' freedoms (Greenwald, 2014, p.96). These programs, frequently defended on the grounds of national safety, can potentially be misused to stifle opposition, regulate information, and influence public sentiment.

In conclusion, data collection in the digital era represents a new form of the Panopticon, where the unseen observer is omnipresent, powerful, and capable of profound privacy invasions. As such, it is crucial to reassess our understanding of privacy and develop robust mechanisms to regulate data collection, ensuring that the power of the digital Panopticon is checked and balanced.

In the vast panorama of the surveillance society, two countries stand out starkly, China and the United Kingdom, each a paragon of a particular strain of surveillance philosophy. The former, a beacon of state surveillance, the latter, a poster child for liberal democratic oversight, yet both entwined in the tendrils of the Panopticon.

China's surveillance society is a testament to the Panopticon's metamorphosis into an all-encompassing digital entity. The Chinese state's surveillance apparatus, bolstered by the technology of firms like Huawei and SenseTime, is in many ways the epitome of the digital Panopticon. In Xinjiang, for instance, the Uighur population is subjected to an almost constant state of surveillance, with facial recognition cameras at every corner and predictive policing algorithms mining data to predict potential dissent (Mozur, 2019). The government's Social Credit System, a system that, in essence, grades citizens based on their behavior, has been lauded by some as a mechanism to encourage 'trustworthy' behavior, but has also been criticized for its potential to stifle dissent (Creemers, 2018, p. 310).

On the other side of the spectrum, the United Kingdom, although a liberal democracy, has one of the highest densities of CCTV cameras in the world (Norris & Armstrong, 1999, p. 78). This extensive network of cameras, combined with advanced facial recognition technology, has led to concerns about privacy invasions and potential misuse. The UK's Investigatory Powers Act 2016, colloquially known as the 'Snooper's Charter', grants wide-ranging powers to security and intelligence agencies, and police, to intercept and store communications data. Critics argue that these practices are an infringement on civil liberties and that oversight mechanisms, though present, are insufficient (Schneier, 2016).

Despite the stark differences in their political landscapes, both countries are emblematic of Foucault's (1977, p. 201) Panopticon in the digital age, demonstrating how pervasive surveillance can become in different sociopolitical contexts. They illustrate the tension between public safety and privacy, between control and freedom, and the power dynamics that underpin these debates.

The Panopticon's transmutation into a digital entity has facilitated an unprecedented level of surveillance. Whether this is a mechanism for societal control or a tool to ensure public safety is a matter of perspective, colored by the political, cultural, and ethical contexts of each society. Yet, it remains undeniable that the Panopticon's omnipresent gaze has taken on a new form, one that is unseen yet ubiquitous, and one that continues to shape and be shaped by the societies it observes.

The Politics of the Panopticon: Surveillance as a Mechanism of Political Control

Authoritarian Panopticon: Surveillance in Autocratic Regimes

In the heart of authoritarian regimes worldwide, we find the Panopticon's embodiment in its most ominous form. Surveillance in autocracies is no longer a tool, but a cornerstone of power, designed to discipline, control, and maintain the status quo (Zuboff, 2019, p. 88). As we delve deeper into this abyss, we witness an intricate architecture of surveillance that, akin to Foucault's Panopticon, leaves no room for evasion.

China serves as a quintessential example of such regimes, employing an expansive surveillance system, the so-called "Golden Shield Project." This project, encompassing a mass surveillance and censorship program, has strategically employed the internet as an instrument of control (Deibert, 2013, p. 65). Deibert (2013) contends that the project's underlying principle is reminiscent of the Panopticon, insofar as it aims to instill self-censorship among citizens through perpetual surveillance.

The scope of surveillance extends far beyond digital territories. Social Credit System (SCS), a Chinese government initiative, is a tool designed to rate the trustworthiness of its citizens, thereby influencing their behavior (Kostka, 2019, p. 58). This system, by assigning scores to individuals based on their conduct, materializes the

essence of the Panopticon by transforming citizens into their own surveillants, thereby instilling discipline (Kostka, 2019, p. 63).

Turning our gaze towards Russia, we find a similar pattern of ubiquitous surveillance. The SORM (System for Operative Investigative Activities) provides Russian authorities with unbridled access to all forms of communication, making privacy an elusive concept (Soldatov & Borogan, 2015, p. 105). The system's omnipresence and the awareness thereof have inculcated a climate of fear and self-censorship among the populace.

However, it would be remiss to suggest that surveillance in autocratic regimes is confined to digital spaces. A stark manifestation of physical surveillance can be seen in North Korea, where local neighborhood units, known as "inminban," keep a meticulous watch over the community (Fahy, 2016, p. 42). This grassroots level surveillance, Fahy argues, breeds a culture of fear and obedience that aligns perfectly with the Panopticon's disciplinary objectives.

In conclusion, the authoritarian Panopticon embodies a comprehensive network of surveillance, meticulously designed to control and manipulate the populace. It transcends the boundaries of digital and physical spaces and, by promoting a culture of self-surveillance and discipline, amplifies the power held by the autocratic regime.

Democratic Dilemmas: Surveillance in Liberal Democracies

The democratic tradition cherishes individual liberties, the rule of law, and privacy, yet the growth of surveillance technologies poses a quandary for these liberal democracies (Lyon, 2001, p.78). The promise of enhanced security and the prevention of crime and terrorism is an attractive proposition, yet this seemingly comes at the expense of the privacy and freedom democracies are built upon.

In the United States, the Patriot Act of 2001, passed in the wake of the 9/11 attacks, substantially expanded the surveillance powers of law enforcement and intelligence agencies (Friedman & Schulzke, 2017, p.45). Under the guise of national security, the Act allowed for widespread data collection and wiretapping, sparking fierce debate about the erosion of civil liberties and privacy.

In a similar vein, the United Kingdom's Investigatory Powers Act of 2016, dubbed the 'Snooper's Charter' by critics, granted unprecedented powers to law enforcement and intelligence agencies to intercept and retain communication data (Bernal, 2016, p. 172). The Act was challenged in the European Court of Human Rights, illustrating the tension between security concerns and the protection of individual rights in democratic states.

The case of Edward Snowden, a former National Security Agency contractor, brought the magnitude of surveillance in democratic societies to light. His revelations about the PRISM program, a clandestine mass electronic surveillance data mining program, ignited a global debate about privacy, surveillance, and the reach of intelligence agencies (Greenwald, 2014, p. 128).

Such practices are not confined to the West. The Aadhaar program in India, a 12-digit unique identity number based on biometric and demographic data, has been widely criticized for its potential for mass surveillance and violation of privacy rights (Bhatia, 2017, p. 301). The program demonstrates how digital technologies are reshaping the balance between the state and the individual in democracies around the world.

These cases illustrate a fundamental dilemma for liberal democracies: how to balance the demands of national security and the prevention of crime with the protection of individual liberties and privacy. This dilemma is not new; it has been a recurrent theme in democratic theory and practice. Yet, the advent of digital technologies has given it a new urgency and complexity.

Democratic societies are grappling with this challenge in different ways. Some, like Germany and the Netherlands, have strong legal protections for privacy and have been resistant to encroachments by surveillance technologies (Koops, 2017, p. 120). Others, like the United States and the United Kingdom, appear to have accepted a greater degree of surveillance as a necessary evil in the fight against crime and terrorism. Yet others, like India, are still wrestling with the implications of digital technologies for their democratic institutions and traditions.

The endeavor to strike a balance between safety and personal privacy in this digital epoch is a decisive challenge for democratic societies in the 21st century. The approach taken to confront this issue will mold the future of democratic administration and the

rights and liberties of individuals. As articulated by Foucault (1977, p. 201), the Panopticon is more than merely a symbol; it is a mechanism of power deeply entrenched in our societal and political existence. Its implications for democracy are substantial and pervasive.

However, democratic societies hold a unique ability for self-amendment and rejuvenation. The ongoing discourse surrounding surveillance is evidence of this ability. As this conversation progresses, it is vital to acknowledge that the Panopticon represents a decision rather than an inevitable outcome, and the equilibrium between safety and privacy is not a situation with winners and losers, but rather a matter of democratic principles, rights, and obligations.

Internalizing the Panopticon: Self-Surveillance and Discipline in Modern Society

As we navigate our way into this digital panopticon, the psychological impacts of self-surveillance are becoming increasingly prominent. The notion of the "watched self" is deeply entrenched in today's society, particularly with the rise of social media platforms where users voluntarily document their lives in a public arena (Rainie & Wellman, 2012, p.101).

Drawing on Foucault's (1977, p.201) ideas about the panopticon and self-discipline, it can be argued that this self-surveillance has led to a culture of self-censorship and performance. The constant awareness of being observed, or potentially observed, leads individuals to modify their behaviors according to societal norms and expectations, a phenomenon outlined by Goffman's (1956, p.2) dramaturgical approach. This shift towards self-censorship and performance is not solely driven by external surveillance mechanisms, but also by the internalized expectations of the audience (Turkle, 2011, p.260).

In addition to self-censorship, the "watched self" incites an internal pressure to curate an idealized self-image (Zhao, Grasmuck, & Martin, 2008, p.1818). Social media, in particular, promotes the construction and maintenance of a meticulously managed 'online self,' often portraying a more positive, successful, and attractive life than the user may actually experience (Manovich, 2013, p.5). This curation process can lead to

psychological distress, such as feelings of inadequacy and low self-esteem, particularly when individuals compare their 'offline selves' with the 'online selves' of others (Fardouly et al., 2015, p.447).

Moreover, self-surveillance fosters a continuous state of alertness, where individuals are perpetually conscious of their actions and behaviors (Marwick, 2012, p.380). This constant state of self-monitoring can be mentally exhausting, leading to anxiety and stress (Bauman & Lyon, 2013, p.23). It can also limit the scope for spontaneity and authenticity, as individuals are constantly 'on guard,' adjusting their behaviors to align with societal expectations (Marwick, 2012, p.379).

Lastly, there is a growing body of research suggesting that excessive self-surveillance may lead to narcissistic tendencies (Buffardi & Campbell, 2008, p.1307). The ability to curate one's online persona, coupled with the potential for constant validation through likes and comments, can foster narcissistic behaviors such as self-promotion and attention-seeking (Bergman et al., 2011, p.358).

The psychological impacts of self-surveillance are complex and multifaceted, manifesting in various ways depending on individual and societal contexts. As we continue to grapple with the implications of our digital panopticon, it is crucial to consider these psychological consequences and how they shape our modern societal interactions.

The internalization of surveillance transcends the personal realm and permeates societal structures, thus shaping our contemporary social milieu. The intertwining of self-surveillance and societal discipline has been extensively studied, and scholars such as Andrejevic (2007) and Haggerty (2006) have meticulously articulated the societal ramifications of self-discipline. As they have compellingly argued, the panopticon's ghost does not merely linger in the corridors of prisons and asylums; it has crept into our homes, schools, workplaces, and, most significantly, our minds.

Self-discipline, fostered by self-surveillance, inadvertently becomes a powerful tool for social control. Foucault (1977) posited that self-discipline is born out of the fear of deviating from social norms and the resultant societal punishment. We are, as Bauman (2000, p. 31) poignantly described, "simultaneously the overseers and the objects of

control," and this has far-reaching implications for societal cohesion and individual freedom.

As sociologist Shoshana Zuboff (2019) has illustrated in her comprehensive study, "Surveillance Capitalism," the self-disciplined citizen becomes an essential cog in the wheel of the capitalist machinery. Paradoxically, the individual who tirelessly works towards self-improvement, thereby conforming to societal norms and ideals, becomes a pawn in a larger economic game. Self-surveillance leads to the commodification of personal data, which is subsequently used to manipulate consumer behavior and perpetuate capitalist structures.

Furthermore, the normalization of surveillance and self-discipline contributes to the gradual erosion of privacy and personal freedom. Lyon (2007, p. 128) astutely notes that "privacy is in danger of being reduced to a luxury item," available only to those who can afford to evade surveillance. This could potentially exacerbate social inequalities and create a further divide between the haves and the have-nots.

In addition, the societal consequences of self-discipline and self-surveillance manifest in the form of conformity and homogeneity. As individuals continuously regulate their behavior in adherence to societal norms, diversity and individuality may gradually diminish. As Marx (2002, p. 18) warns, we might unwittingly be moving towards a "monolithic society," characterized by uniformity and a lack of dissent.

To conclude, the panopticon's power no longer resides solely in its architectural design or the pervasive gaze of the watcher. It resides within us, subtly shaping our actions, thoughts, and societal structures. While surveillance technology and mechanisms have undeniably brought significant benefits, it is crucial to critically examine their potential drawbacks and ethical implications. As we traverse this age of surveillance, we must continually question the societal costs we are willing to pay for security and conformity.

The Digital Panopticon: Social Media as a Platform for Surveillance

An intriguing transformation of the digital age is the voluntary exhibitionism that manifests itself in the use of social media. This section navigates the concept of voluntary exhibition as an aspect of modern surveillance, marked by incessant information sharing

on social platforms. Social media platforms are akin to a modern digital Panopticon, allowing for constant surveillance; however, the difference lies in the voluntary nature of this surveillance. We expose ourselves and our lives willingly, seeking visibility and validation in a vast digital crowd (Fuchs, 2017, p.78). This is not Foucault's Panopticon, it is our own self-constructed digital surveillance system.

The ability to 'share' and 'like' has become a new form of social currency. The more likes, shares, and followers one has, the more social value one seemingly possesses (Marwick, 2012, p. 378). This has created a culture of constant self-presentation and self-surveillance, where users, in a bid to gain more social value, continuously monitor and curate their online image.

This phenomenon is excellently analyzed by Alice Marwick and Danah Boyd in their work, "I tweet honestly, I tweet passionately" (2011, p.114). They argue that Twitter's architecture of visibility encourages a form of 'micro-celebrity' culture, where users adopt a public persona, strategically revealing personal details to create a certain image.

A survey conducted by Pew Research Center in 2019 revealed that 72% of U.S. adults use at least one social media site, with the average user spending approximately 2 hours and 22 minutes per day on these platforms (Perrin & Anderson, 2019, p. 16). This extensive use and exposure has profound implications for privacy, data protection, and individual autonomy.

The paradox is that while we decry the invasive surveillance of the state or corporations, we willingly participate in a form of surveillance that arguably strips us of our privacy more than any government entity could. The issue of data protection also arises. As we share our lives online, we provide a treasure trove of data, ripe for exploitation by companies for targeted advertising, a process termed as 'surveillance capitalism' by Shoshana Zuboff (2019, p. 8).

The Digital Panopticon is an embodiment of sophisticated mechanisms and their tentacles reach even deeper with the introduction of algorithmic surveillance. Algorithmic surveillance, a technology that is enmeshed with the daily operations of social media

platforms, epitomizes the culmination of Bentham's vision in the digital age (Zuboff, 2019, p. 14).

In the online world, users' behavior, preferences, and engagements are monitored, collected, and analyzed to create personalized experiences. The 'like' button on Facebook, for instance, is not merely a tool for social interaction. It serves a dual function as a data collection point, feeding into the vast databases that form the backbone of algorithmic surveillance (Fuchs, 2017, p. 68). Every click, share, comment, and even time spent hovering over a post, contributes to an ever-growing digital profile of the user, a profile employed for targeted advertising and manipulation.

Algorithmic surveillance is not a passive observer in the digital Panopticon. It influences user behavior and transforms the digital landscape. Eli Pariser (2011, p. 15), in his seminal work "The Filter Bubble," describes how personalization algorithms create echo chambers, limiting exposure to contrasting views and reinforcing existing beliefs. This algorithmic control harkens back to Foucault's (1977, p. 202) concept of discipline without the need for physical coercion.

However, the implications of algorithmic surveillance are not confined to the individual's digital experience. They permeate the societal fabric, giving rise to new forms of power dynamics. Andrejevic (2013, p. 12) argues that algorithmic surveillance contributes to a 'surveillance divide,' where those with access to and control over data hold power over those who are the subjects of data. This is a profound shift in the balance of power, with the watched becoming increasingly powerless against watchers armed with sophisticated algorithms.

Furthermore, the pervasiveness of algorithmic surveillance has given birth to novel forms of exploitation. Shoshana Zuboff (2019, p. 24) coined the term 'surveillance capitalism' to describe an economic system in which personal data is the new commodity. Users, in their quest for connection and communication, offer up their data in exchange for 'free' services, unaware of the hidden cost.

Navigating the Ethical Labyrinth: The Panopticon and the Quest for Privacy

As we navigate the interstices of the panoptic society, it is crucial to examine the sanctity of privacy and its attendant rights, as well as the implications of surveillance on

these rights. Our exploration starts with Westin's (1967) seminal work on privacy, where he envisions privacy as the right of the individual to determine the extent of personal information shared with others (Westin, 1967, p. 7). However, the complexity and nuances of privacy have only amplified in the digital age, with the advent of technology and the internet facilitating an unprecedented intrusion into personal lives.

Solove (2008) puts forth an insightful perspective in his critique of the traditional concept of privacy, arguing that the old dichotomy of private vs. public is an inadequate framework in the digital era. The reason, he postulates, lies in the fact that the internet has blurred these boundaries, rendering the distinction obsolete (Solove, 2008, p. 101). This argument forms a compelling starting point for rethinking the concept of privacy in our current socio-technological context.

In addition to the theoretical reconceptualization of privacy, the practical realities of surveillance have also posed significant challenges. This is reflected in Snowden's (2019) revelations about the extensive surveillance programs operated by the National Security Agency in the United States, which shocked the world and raised critical questions about the balance between national security and individual privacy (Snowden, 2019, p. 235).

These revelations have led to numerous debates about the ethical implications of surveillance and the erosion of privacy. Lyon (2018) argues that surveillance has become a social sorting mechanism that categorizes individuals based on their data profiles (Lyon, 2018, p. 82). In this context, the right to privacy transcends personal boundaries and seeps into issues of social justice and equality.

Moreover, the European Union's General Data Protection Regulation (GDPR) has been a significant step in fortifying privacy rights, setting a precedent for other regions. The GDPR underscores the 'right to be forgotten,' giving individuals the power to have their data deleted (EU GDPR Information Portal, 2020).

This discussion inevitably leads us to the heart of the ethical labyrinth: is there a right to hide in this age of surveillance? What constitutes an acceptable level of privacy, and who decides this? The answers are complex and multifaceted, but one thing remains

clear - the quest for privacy in the panoptic society is an ongoing struggle that demands our constant attention and critical engagement.

The intricate tapestry of surveillance and freedom, where the threads of legality and ethics intersect, forms a conundrum that societies grapple with in the age of the digital panopticon. The question at the core of this issue is how far can the state's surveillance powers extend without encroaching upon individual freedoms? As Lyon (2001, p.67) articulates, "surveillance is not merely a matter of personal invasion but is tied to the management and control of modern organizations and institutions."

The growing prevalence of surveillance technology presents potential conflicts between public safety and individual rights. The legal precedents set by cases such as Kyllo v. United States (2001), wherein law enforcement's use of a thermal imaging device to scan a home without a warrant was ruled unconstitutional, exemplify these tensions (Kerr, 2007, p.833). The ruling underscored the right to privacy as integral to the protection of individual freedom, reinforcing the Fourth Amendment's safeguard against unreasonable searches and seizures.

Furthermore, the rapid evolution of surveillance technology often outpaces the development of legislation, leading to a legal grey area. In an increasingly interconnected world, data flows across national boundaries, further complicating the legal landscape. As stated by Deibert and Rohozinski (2010, p.15), "the jurisdictional maze of international cyber surveillance poses significant challenges to any conventional legal approach."

However, the ethical dimension of this conundrum extends beyond the legal sphere. The constant gaze of the digital panopticon, as Bauman (2000, p.81) suggests, can lead to the "diminution of human autonomy and dignity," posing a threat to democratic values. The right to privacy, as Warren and Brandeis (1890, p.193) argued, is "the most comprehensive of rights and the right most valued by civilized men," a sentiment echoed by contemporary scholars.

In the context of Foucault's panopticon, the balance between surveillance and freedom transforms into a discussion on power dynamics. As Foucault (1977, p.201)

posits, surveillance is a manifestation of power, and therefore, the question of surveillance is intrinsically a question of how power should be exercised, checked, and balanced.

Tomorrow's Panopticon: Potential Technological Advancements

As we look forward, the architecture of the Panopticon, conceived by Bentham and expanded upon by Foucault, is increasingly realized in the technological advancements of the digital age. These tools, while they hold promises for streamlining communication and enabling global connectivity, also extend the reach and effectiveness of surveillance (Lyon, 2001, p. 33).

Artificial Intelligence (AI) stands as a prominent development in surveillance capabilities. As Zuboff (2019, p. 264) illustrates, AI technologies are now capable of processing vast amounts of data to make predictions about human behavior. These predictions can be used to manipulate consumer behavior, control dissent, or enable state surveillance. The advent of facial recognition technology, for instance, provides a disturbingly literal representation of the Panopticon's all-seeing eye. This technology, already deployed in cities like London and Beijing, allows for constant monitoring and identification of individuals in public spaces (Harcourt, 2015, p. 95).

The ubiquity of smartphones and Internet of Things (IoT) devices also expands the possibilities for surveillance. These devices, constantly collecting data about their users, form a network of digital observers, a new kind of Panopticon that surveils not just our physical actions, but our digital ones as well (Howard, 2015, p. 21). As Andrejevic (2005, p. 211) points out, these devices track our location, monitor our interactions, and even record biometric data, contributing to the formation of a comprehensive digital profile.

Perhaps even more concerning is the potential for self-surveillance offered by these technologies. As Bauman and Lyon (2013, p. 78) suggest, we willingly participate in our own surveillance, sharing personal information and life updates on social media platforms, tracking our fitness and health metrics with wearable devices, and allowing our smartphones to record our location and behavior patterns. This digital self-monitoring, reminiscent of Foucault's self-discipline, has become an accepted part of modern life.

While these technological advancements hold enormous potential for convenience and efficiency, they also pose significant challenges to privacy and individual freedom. The digital Panopticon is not a future possibility but a present reality, and its gaze is fixed squarely on us. The question, then, is not whether we will live under surveillance, but how we will navigate the new landscapes of visibility and control these technologies create (Haggerty & Ericson, 2000, p. 611).

As we venture into this brave new world, we must grapple with the ethical and legal implications of these technologies. The Panopticon's watchful eye is no longer a metaphor but a literal reality, and its gaze is unblinking. How we respond will shape the contours of our digital future. As we gaze into the future, we must consider the potential metamorphoses of surveillance and control in the emerging socio-technological realities. The prospect of new disciplines prompted by the advancement of surveillance technologies could usher in a new epoch in societal regulation (Zuboff, 2019, p. 88).

One such discipline poised to gain prominence in the future is biometric surveillance. The use of unique biological traits for identification and tracking is not new; however, emerging technologies could drastically augment its capabilities (Mordini & Massari, 2008, p. 456). Facial recognition technology, for instance, is now capable of identifying individuals in crowds with astonishing accuracy. The technology's prospective improvements promise an omnipresent eye, ever watchful, recognizing and registering each face in real-time (Gates, 2011, p. 138). This technology's expansion into public spaces, like airports and shopping malls, exemplifies the increasing normalization of surveillance in our daily lives.

Another discipline on the horizon is predictive policing, a practice that uses data analysis to predict potential criminal activity (Ferguson, 2017, p. 93). By analyzing patterns in historical crime data, law enforcement agencies can allocate resources more efficiently. However, there is a fine line between predictive policing and 'pre-crime', a concept popularized in science fiction, where individuals are punished based on the statistical likelihood of their committing a crime. The ethical implications of this approach are deeply concerning and warrant vigilant scrutiny.

In tandem with these technologies, we may also witness a rise in algorithmic governance, where decision-making processes are automated using complex algorithms

(Danaher, 2016, p. 25). This may create a new form of discipline where an individual's behavior is regulated not just by human overseers but by impersonal and inescapable algorithms. The impact on personal freedom and autonomy could be substantial.

The dawn of quantum computing, with its potential for unprecedented data processing capabilities, could further amplify the reach and efficiency of these disciplinary mechanisms (Preskill, 2018, p. 79). The ability to process vast amounts of data simultaneously could make the surveillance system more pervasive and efficient, thus intensifying the panoptic gaze.

In conclusion, the future of surveillance and discipline could be characterized by an amalgamation of advanced technologies. These could redefine the landscape of control, making the panoptic gaze more penetrating and inescapable than ever before. However, the ethical implications of these advancements necessitate a careful, critical analysis to ensure that the march of progress does not trample upon our fundamental rights and freedoms (Nissenbaum, 2004, p. 100).

Conclusion: Reimagining the Panopticon in a Surveillance-Driven World

The Panopticon, as conceptualized by Jeremy Bentham and further elaborated by Michel Foucault, has seemingly evolved from a theoretical construct into a tangible reality of the contemporary world. In this surveillance-driven era, the principles of the Panopticon permeate various aspects of our society, from the realm of digital communication to the global political order.

Throughout this article, the exploration of the Panopticon's application and implications has indeed been a journey across disciplines, geographies, and epochs. We navigated the labyrinth of ethics and legality surrounding privacy and surveillance, unearthing a multitude of perspectives that both challenge and affirm the Panopticon's place in our society. Amid a world where surveillance has become ubiquitous, the concept of privacy is incessantly redefined and contested. The competing narratives of ensuring security and preserving freedom present a legal and ethical conundrum that continues to incite scholarly debates.

The advent of modern technologies, particularly in the field of digital communication, has further amplified the Panopticon's influence, making its presence

more pervasive and its gaze more penetrating. While these advancements promise unparalleled convenience and connectivity, they also bear the risk of establishing a state of perpetual surveillance, thus redefining discipline and control in the process.

The Panopticon, however, is not an unchanging, monolithic structure. It is subject to evolution and reinterpretation, capable of spawning new forms of discipline and surveillance that might surpass our current understanding. As we gaze into the future, it is crucial to consider how the Panopticon might adapt to, and even shape, the technological advancements and societal shifts on the horizon.

In closing, the Panopticon serves as a compelling lens through which we can scrutinize the ongoing tussle between surveillance and privacy, control and freedom, technological advancement, and ethical considerations. Reimagining the Panopticon in our contemporary world is not merely an intellectual exercise, but an imperative for understanding and navigating the complexities of our surveillance-driven society. This understanding is essential for those who desire to shape a future where technology serves humanity without curtailing its fundamental freedoms.

The discourse on the Panopticon is far from over. As our world continues to evolve and as surveillance technologies grow more sophisticated, the Panopticon may yet reveal other facets of its influence. We must, therefore, remain vigilant, critical, and adaptive, ready to meet the challenges and seize the opportunities that such changes might bring.

References

Andrejevic, M. (2005). "The work of watching one another: Lateral surveillance, risk, and governance". *Surveillance & Society*, 2(4), 479-497.

Andrejevic, M. (2007). "Surveillance in the Digital Enclosure". *The Communication Review*, 10(4), 295-317.

Andrejevic, M. (2013). *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York, NY: Routledge.

Bauman, Z. (2000). *Liquid Modernity*. Polity Press.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity.

Bentham, J. (1791). *Panopticon; or The Inspection-House*. London: T. Payne.

Bentham, J. (1995). *The Panopticon Writings*. London: Verso.

Bergman, S. M., Fearrington, M. E., Davenport, S. W., & Bergman, J. Z. (2011). "Millennials, narcissism, and social networking: What narcissists do on social networking sites and why". *Personality and Individual Differences*, 50(5), 706-711.

Bernal, P. (2016). "Data gathering, surveillance and human rights: recasting the debate". *Journal of Cyber Policy*, 1(2), 243-264.

Bhatia, G. (2017). "The Aadhaar Scheme: A Constitutional and Human Rights Analysis". In S. S. Wadhwa (Ed.), *The Future of Indian Economy: Past Reforms and Challenges Ahead* (pp. 301-328). New Delhi, India: Yash Publications.

Buffardi, L. E., & Campbell, W. K. (2008). "Narcissism and social networking web sites". *Personality and Social Psychology Bulletin*, 34(10), 1303-1314.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *The Guardian*. Retrieved Jan 10, 2023, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

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

Danaher, J. (2016). "The threat of algocracy: Reality, resistance and accommodation". *Philosophy & Technology*, 29(3), 245-268.

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto, Canada: Signal.

Deibert, R. J., & Rohozinski, R. (2010). "Liberation vs. control: The future of cyberspace". *Journal of Democracy*, 21(4), 43-57.

Deleuze, G. (1992). "Postscript on the Societies of Control". *October*, 59, 3-7.

EU GDPR Information Portal. (2020). *Key Changes with the General Data Protection Regulation*. Retrieved Apr 12, 2023, from https://eugdpr.org/the-regulation/

Fahy, S. (2016). *Marching through Suffering: Loss and Survival in North Korea*. New York, NY: Columbia University Press.

Fardouly, J., Diedrichs, P. C., Vartanian, L. R., & Halliwell, E. (2015). "Social comparisons on social media: the impact of Facebook on young women's body image concerns and mood". *Body Image*, 13, 38-45.

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York, NY: NYU Press.

Friedman, B., & Schulzke, M. (2017). *The Ethics of Surveillance: An Introduction*. New York, NY: Routledge.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Fuchs, C. (2017). *Social media: A critical introduction*. London, UK: Sage.

Fussey, P., & Murray, D. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. London: University of Essex Human Rights Centre

Galloway, A. R. (2012). *The Interface Effect*. Cambridge: Polity.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York, NY: NYU Press.

Gill, M., & Spriggs, A. (2005). *Assessing the Impact of CCTV*. London: Home Office Research, Development and Statistics Directorate.

Goffman, E. (1956). *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.

Goold, B. J. (2004). *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books.

Haggerty, K. D. (2006). "Tear down the walls: on demolishing the panopticon". In D. Lyon (Ed.), *Theorizing surveillance: the panopticon and beyond* (pp. 23-45). Cullompton, UK: Willan Publishing.

Haggerty, K. D., & Ericson, R. V. (2000). "The surveillant assemblage". *The British Journal of Sociology*, 51(4), 605-622.

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

Howard, P. N. (2015). *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven, CT: Yale University Press.

Introna, L. D., & Wood, D. M. (2004). "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems". *Surveillance & Society*, 2(2/3), 177-198.

Jenkins, R., & Carle, C. (2011). "Recognition is Not Recognition is Not Recognition". In A. Calder, G. Rhodes, & M. Johnson (Eds.), *Oxford Handbook of Face Perception* (pp. 209-224). Oxford: Oxford University Press.

Kerr, O. S. (2007). "Searches and seizures in a digital world". *Harvard Law Review*, 119(2), 531-585.

Koops, B. J. (2017). "The trouble with European data protection law". *International Data Privacy Law*, 4(4), 250-261.

Kostka, G. (2019). "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval". *New Media & Society*, 21(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (2006). *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge, UK: Polity Press.

Manovich, L. (2013). *The language of new media*. Cambridge, MA: MIT press.

Marx, G. T. (2002). "What's new about the "new surveillance"?". *Surveillance & Society*, 1(1), 9-29.

Marwick, A. (2012). "The public domain: Social surveillance in everyday life". *Surveillance & Society*, 9(4), 378-393.

Marwick, A. E., & Boyd, D. (2011). "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience". *New Media & Society*, 13(1), 114-133.

McCahill, M., & Norris, C. (2002). "CCTV in Britain". *Urban Eye Report*, 2, 1-61.

Mordini, E., & Massari, S. (2008). "Body, biometrics and identity". *Bioethics*, 22(9), 488-498.

Mozur, P. (2019, April 14). "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority". *The New York Times*. Retrieved Feb 19, 2023, from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Nissenbaum, H. (2004). "Privacy as contextual integrity". *Washington Law Review*, 79(1), 119-158.

Norris, C., & Armstrong, G. (1999). *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Pariser, E. (2011). *The Filter Bubble: What the Internet is Hiding From You*. New York, NY: Penguin Press.

Perrin, A., & Anderson, M. (2019). *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018*. Washington, D.C: Pew Research Center.

Preskill, J. (2018). "Quantum Computing in the NISQ era and beyond". *Quantum*, 2, 79.

Rainie, H., & Wellman, B. (2012). *Networked: The new social operating system*. Cambridge, MA: MIT Press.

Ramzy, A., & Buckley, C. (2019, April 14). "China Uses DNA to Track Its People, With the Help of American Expertise". *The New York Times*. Retrieved Apr 08, 2023, from Https://www.nytimes.com/2019/04/14/world/asia/china-xinjiang-uighur-dna-thermo-fisher.html

Schneier, B. (2016, November 26). "The UK's New Surveillance Law Is a Stalker's Dream". *Motherboard*. Retrieved May 10, 2023, from

https://motherboard.vice.com/en_us/article/wnx8yy/the-uks-new-surveillance-law-is-a-stalkers-dream

Semple, J. (1993). *Bentham's Prison: A Study of the Panopticon Penitentiary*. Oxford: Clarendon Press.

Snowden, E. (2019). *Permanent Record*. New York, NY: Metropolitan Books.

Soldatov, A., & Borogan, I. (2015). *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York, NY: PublicAffairs.

Solove, D. J. (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". *San Diego Law Review*, 44, 745-772.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Tene, O., & Polonetsky, J. (2013). "Big Data for All: Privacy and User Control in the Age of Analytics". *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239-273.

Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York, NY: Basic Books.

Warren, S. D., & Brandeis, L. D. (1890). "The Right to Privacy". *Harvard Law Review*, 4(5), 193-220.

Westin, A. F. (1967). *Privacy and Freedom*. New York, NY: Atheneum.

Zhao, S., Grasmuck, S., & Martin, J. (2008). "Identity construction on Facebook: Digital empowerment in anchored relationships". *Computers in Human Behavior*, 24(5), 1816-1836.

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