THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

SP499: Dissertation - International Social & Public Policy

SUMMATIVE SUBMISSION TEMPLATE

CANDIDATE NUMBER: *(**Five-digit number** available via LSE for You – this is not the same as the number on your LSE ID card!)*	**2 3 0 1 8**
COURSE CODE:	**SP499**
PROGRAMME STREAM:	**General**
ASSESSMENT TITLE:	How well does the GDPR empower employees in the face of modern workplace surveillance?
WORD COUNT: *Excludes references and appendices.*	**9917**

‘I have completed the LSE ethics review and my project was approved ☐ or approval was not needed ☒’
Tick as required.

*Please tick this box if you **DO NOT** want your assessment to be shared with future cohorts:* ☐

Sample dissertation work is frequently requested by students each year and It is helpful for students to be able to learn from previous students’ dissertations [through our dissertation archive on Moodle]. Your work will only be shared as examples and for learning purposes. Your willingness to help future students in the Department is appreciated.

Enabling the Panpoticon?
GDPR, Employee Power, and Workplace Surveillance

August 2024

The advent of machine learning (ML) surveillance systems has raised significant ethical and legal concerns regarding employee privacy and autonomy in the workplace. This study examines the implications of digital surveillance on employee power dynamics, with a particular focus on the European Union's General Data Protection Regulation (GDPR). Using Foucault's Panopticon and theories of disciplinary power and biopower, the research analyzes how modern surveillance practices reinforce employer control and diminish employee agency. Through a critical review of existing literature, case studies involving Amazon France Logistique and H&M, and an exploration of GDPR's legal framework, this study evaluates the regulation's effectiveness in curbing excessive surveillance and protecting employee rights. The findings highlight the limitations of the GDPR in addressing the complex challenges posed by ML-enhanced surveillance, emphasizing the need for more robust legal protections and policy developments to safeguard employee dignity and autonomy in the digital workplace.

1 Introduction

Monitoring, categorizing, and profiling employees has never been easier. The increasing adoption of digital surveillance, coupled with new powerful machine learning (ML) algorithms, is fundamentally shifting how employers track their workforce across every industry. Machine learning surveillance systems are automated technologies that use algorithms to analyze large datasets, often collected through digital monitoring, to identify patterns and make decisions about individuals or groups (Buchanan, 2020). These systems work by training models on historical data to recognize specific triggers or anomalies, enabling continuous, real-time surveillance with minimal human intervention. The use of these technologies varies across workplaces, but it is often used to infer the thoughts, feelings, and behaviors of employees through wearable biometric devices and 'sentiment analysis' of video recordings (Ball, 2021). Just as common, employers use it to keep tabs on location and task-completion through similar means like video but also through GPS systems and digital workspaces (Holland, Cooper, & Hecker, 2015). The implementation of digital surveillance is a loop that creates an instrument of power for employers. The algorithms that enable the technology to predict worker behavior require data to base the predictions on; therefore, the more the technology is used the more data it aggregates and the better it can provide employers with analytics. Such technologies present a critical challenge for regulators: How can ML-enhanced surveillance technologies, which diminish the role of human judgment and analytic processes, be restructured to reinforce employee autonomy and privacy, rather than serving as tools of control and subjugation? Can these technologies, initially developed to maximize efficiency and security, be reimagined to foster employee well-being, build trust, and promote a positive work environment while maintaining their intended benefits? If such a transformation is not feasible, what do these technologies signify for the broader power dynamics and social structures within the workplace? How can regulations be strengthened to ensure these technologies not only secure the workplace but also safeguard employee agency and civil rights?

I tackle these questions by exploring the General Data Protection Regulation (GDPR), a landmark in global data protection legislation which aims to harmonize data privacy laws across Europe and empower individuals with greater control over their personal information. As digital technologies become increasingly pervasive in the workplace, the GDPR's impact on employee surveillance has garnered significant attention. The regulation sets out stringent requirements for data processing, emphasizing principles such as transparency, data minimization, and accountability, which are intended to safeguard employees' privacy and autonomy. However, the effectiveness of the GDPR in balancing the power dynamics between employers and employees remains a contentious issue. This paper examines the GDPR's role in regulating workplace surveillance, focusing on its ability to protect employees' rights and limit the scope of employer power. This research explores the challenges and limitations of the GDPR in addressing the evolving landscape of digital surveillance and its implications for employee autonomy. Ultimately, I answer this paper's driving research question: How well does the GDPR empower employees in the face of modern workplace surveillance? The findings highlight the need for a more nuanced understanding of how the GDPR operates in practice and the potential for further legal and policy developments to enhance its effectiveness in the context of workplace surveillance.

I begin with a literature review discussing the contours of modern workplace surveillance and its implications for employee power. Then, I move to describe my research methodology and introduce the study in five sections: (1) an overview and analysis of the GDPR's proportionality and necessity requirements; (2) a case example involving Amazon France; (3) an analysis of the effectiveness of GDPR enforcement; (4) an overview and analysis of the GDPR's consent requirements; and (5) a case example involving H&M. My findings are discussed in terms of Foucault's panopticon and conceptions of power. Finally, I present policy recommendations for European Union member states moving forward. This study adds value to existing research by contextualizing Foucault's theories within the modern context of digital workplace surveillance within the European Union. It bridges historical and modern perspectives, highlighting the evolution of surveillance from traditional methods to sophisticated digital monitoring, showing the continuity and transformation of surveillance practices over time.

2 Literature Review

This literature review aims to contextualize the study by exploring core themes in existing literature on surveillance and employee power, specifically focusing on Foucault's Panopticon, and connecting these theories to the modern employer-employee dynamics. Additionally, it will examine current legal frameworks in the United States and European

Union to understand existing regulations on workplace surveillance. The implications that are drawn from the theoretical perspectives on surveillance will be discussed to argue the continued relevance of Foucault's work. For the purposes of this paper, we will use David Lyon's definition of surveillance: "any collection and processing of information, whether personally identifiable or not, for the purposes of influencing or managing those whose data have been garnered"(Ball, 2021). An act of surveillance thus involves the intentional gathering of information about another person, in this case an employee.

2.1 Historical and Theoretical Foundations

From the 'Scientific Management' theories of Fredrick Taylor in the 1880s to Henry Ford's assembly line in the 1920s to the rise of CCTV in the 1970s, scholars have reflected on the potential of new technologies as an affordance for exercising power on laborers. Michel Foucault's notions of power, the primary theory referenced throughout this paper's later discussion, is ever present in much of digital surveillance scholarship today. This is especially true regarding his ideas on the interiorization of employer norms through the reconceptualization of Jeremy Bentham's "Panopticon" (Bentham, 1962). The Panopticon was a prison design that allowed a single guard to observe all inmates without the inmates being aware of the observation. It has three core assumptions: omnipresence of the ward, universal visibility of the prisoner, and prisoners believing they are under constant watch.

Both in public lectures and published works, Foucault used this to serve as a metaphor for the evolution of modern disciplinary institutions, including the workplace (Foucault, 1980, 1985, 2010). He argued observation by employer allows for comparison of employees based on predetermined rules, creating a hierarchy. Observation thus introduces conformity and sets limits to define differences. Specifically, in "Discipline and Punish" (Foucault, 1979), he argued power through surveillance manifests not just through direct repression but through "technology of the self." Those being observed who are cognizant of perpetual surveillance internalize norms set by the observer, thereby conforming to expected behaviors without coercion. Employers can set the rules for what is 'good' or 'bad' behavior, controlling employees as needed and limiting their power. Today, digital performance monitoring can significantly influence a person's perceptions and behavior in the work environment. For example, Stanton and Julian (2002) conducted an experiment in which factory workers were monitored. The workers perceived the monitored tasks as more important, indicating that the monitoring served as a social cue.

2.2 Surveillance and Employee Power

This initially may not come across as an entirely bad thing. Employees can sense what's important to get done, and work harder for a specific task. However, Foucault's Panopticon helps us understand how this exercise of employer power can quickly lead to an abusive environment. He does this with his notion of self-discipline through surveillance. Rosenblat's (2018) study of Uber, for instance, demonstrates how digital surveillance negatively affected the autonomy of its drivers. Some drivers were given priority treatment while others suffered because of Uber's ride-matching algorithm. A critical issue here is the opacity of the algorithms powering the surveillance models, often referred to as "black box" algorithms (Pasquale, 2015), which operate without providing clear information to employees. This lack of transparency forces employees to modify their behavior, not to enhance productivity, but to align with the algorithm's perceived expectations. This often involves employees taking on unpaid or unseen labor, such as adopting different attitudes to please employers or customers (Raval & Dourish, 2016; Gandini, 2016). These dynamics only confirm the panoptic mechanism of Foucault's theories. The employees, aware of being monitored but unaware of how the algorithms work, alter their actions to meet perceived expectations, thereby reinforcing employer control. Continuous self-regulation under surveillance mirrors Foucault's idea that power is most effective when internalized by the subject.

In his work, Foucault categorized two forms of power that operate through the panopticon as 'disciplinary power' and 'biopower'. 'Disciplinary power' is what was just described: the monitoring and normalization of an individual's behavior. This is clearly seen in today's workplace through documentation of action, performance reviews, and surveillance. 'Biopower', on the other hand, is a broader concept that emerged later in Foucault's work. It refers to the control of groups through the administration of life and health processes. It is interesting to note that 'biopower' operates at a broader, group level rather than the individual. However, both are present in the modern workplace. Regarding 'disciplinary power', employers now have the technology necessary to observe and correct any activity they deem unnecessary or unproductive. As an example, Moore, Upchurch, and Whittaker's (2018) study on warehouse employees in the UK showcased that surveillance technology is used to track break times and individual productivity. This has led to the removal of some employees soon after the technology was implemented. Employers' use of algorithmic and data-driven promotion systems can also inadvertently perpetuate discrimination despite intentions to increase efficiency (Rosenblat, Kneese, & Boyd, 2014). These systems often rely on historical data that may contain implicit biases, resulting in the systematic exclusion of certain groups based on race, gender, or socio-economic status. This digital categorization of employees by race, gender, or age is a means of managing the workforce through classification and hierarchy. Mahnoka (2020) highlights the case of Afton Manufacturing, where the manager stated, "employees had a tendency to stretch out breaks sometimes up to 25 or 30 minutes a day, instead of the 20 minutes allocated" prior to the new surveillance methods, but now the technology enables employers to punish those taking ungiven breaks.

This monitoring of the minutiae of employee activity is often attached to a focus on employee health and fitness through corporate 'wellness programs', a direct exercise of 'biopower'. Henry Ford was one of the first who attempted to structuralize 'biopower' in his organization to control employee lifestyles in the early 1900s. He developed a 'Sociology Department' for his company that used intrusive techniques such as home visits to evaluate employee behavior even outside of the factory. Employer 'biopower' today, however, is far greater than in the times of Ford (Ajunwa, Crawford, & Schultz, 2017). Modern options for exercising 'biopower' aren't so constrained by the costs of supporting an entire department. Data gathered from wearable devices and biometric video surveillance is less overtly visible and far cheaper to process and analyze (Rose, 2008; Silverman, Vogt, & Yanowitch, 2016; Moran, 2017). The importance of this lies in its connection to the core principle of self-discipline in the panopticon. Employers incentivize 'moral' and healthy lives through these programs but not to genuinely benefit the employee, often instead to determine eligibility for wage increases and even rank their employability (Manokha, 2020). Thus, their benefit to the company also gets measured by rankings and scores. Employees are then pushed to be both productive but also physically healthy, requiring more modification of that individual's decisions. This could include changing their diet, quitting vaping, or increasing exercise. Thus, digital monitoring significantly impacts employee well-being. The need to modify behavior along with higher work intensity leads to higher stress, burnout, and a variety of health issues (Mulholland & Stewart, 2014). Contemporary monitoring technologies not only enhance the power wielded over workers but also strongly correlate with overworking and elevated stress levels. Understanding how these forms of power manifest, and their impact on employees is essential for analyzing the effectiveness of current policies aimed at empowering employees. Legal frameworks attempt to protect personal data and ensure privacy; however, the extent to which they mitigate the disciplinary and biopower mechanics present, remains the key question.

In sum, the rise of algorithm-driven surveillance has profoundly altered workplace monitoring, making three central assumptions of the panopticon more pertinent for those under surveillance. As research has shown, impact of this new technology extends beyond the core assumptions, as employers increasingly monitor not only productivity but also employee health and fitness. This shift suggests that workplace ’biopower’ is becoming more individualized and disciplinary, and that panoptic characteristics are only becoming more common.

2.3 Other Theories on Surveillance

Foucault’s Panopticon reverses the concept of a traditional dungeon. Where once the darkness and invisibility of prison was the trap, now the visibility becomes the trap. The resulting discipline “makes possible the operation of a relational power that sustains itself by its own mechanisms and which, for the spectacle of public events, substitutes the uninterrupted play of calculated gazes” (Foucault, 1976).

Yet, Foucault’s work is not without fault. It is also possible that the extent to which the panopticon can be applied to digital surveillance today is limited. Many scholars have argued this, abandoning it in favor of other theoretical frameworks potentially better suited. A primary issue with it in the context of this paper is that modern digital surveillance goes beyond the simple observer-subject dynamic. It involves complex data gathering, storage and analysis systems that are not adequately captured by Foucault’s theories as these technologies simply did not exist when the theories were developed. In response to this, Haggerty and Ericson (2000) introduced the idea of ‘surveillant assemblage’, building a framework that reflected a collection of observers functioning together as a whole. It was intended to refer to the interconnected, networked nature of current surveillance systems.

Unlike the Panopticon, which is tied to specific locations like prisons, surveillant assemblage operates across various spaces simultaneously, both physical and virtual. Haggerty and Ericson (2000) also adopted a data-centric approach, focusing on the collection data from individuals' actions profile behavior, very aligned with today's algorithm-powered systems. Does this mean that using Foucault's theories is now both impetuous and anachronistic? Foucault himself was not even considering the emerging surveillance technologies of his time during his work (Wood, 2016). 'Surveillant assemblage' rectifies that, diverging from Foucault in decentralizing the observer by abstracting human bodies from physical spaces, and addressing how contemporary surveillance transforms privacy. It suggests that privacy is now about "the control and flow of personal information in digital environments." However, while Haggerty and Ericson's (2000) work here is successful in offering valuable insights into the nature of surveillance now, I argue it simply does not negate the continued applicability of Foucault's panoptic principles. Despite technological advancements, the psychological impact of observation and the resulting self-regulation remains. Also, the asymmetrical nature of surveillance, where the watchers are unseen, persists. This is evident in both traditional panoptic structures and modern surveillance, where individuals may be unaware of who is collecting data and for what purpose.

Foucault's theories have also been criticized for viewing surveillance as a route to enforce conformity when surveillance in the modern workplace arguably has entirely different goals (Parreno & Demeterio III, 2021). Marxist surveillance theory corrects this, described by Zuboff (2015) as a lens to analyze surveillance practices in the context of class struggle, power dynamics and capitalist exploitation. This perspective views surveillance as a tool used by those in power to maintain managerial control and maximize profit in the capitalist system. It differs from Foucault who focused on power relations and disciplinary mechanisms instead of economic determinism. Marxist surveillance theory can be applied in different ways to workplace surveillance. For example, looking at the working conditions of delivery drivers whose data was tracked to monitor progress in deliveries, Zipperer, McNicholas, Poydock, Schneider, and Harknett (2022) demonstrate how the collection of data allowed for the optimization of the labor process and the extraction of surplus value, aligning with Marx's critique of capitalist exploitation. Another way Marxist surveillance theory is applicable is through the commodification of employee data. The data collected from workers becomes the intellectual property of the employer, making it difficult for employees to leave the company without losing the value they have contributed (Fuchs, 2013). This creates a form of dependency and further consolidates employer power. Indeed, in the case of Ferguson Enterprises in the United States, some evidence suggests that the data collection of employee activities strengthened employer claims on intellectual property and enforcement of non-compete agreements, legally restricting employees' ability to work elsewhere (Osterman Research, 2016).

Despite these valid arguments suggesting Marxist surveillance theory is more useful for examining the dynamics of modern surveillance, I argue for the continued use and relevance of Foucault. Specifically, Foucault's notions of power are still highly applicable. Marxist surveillance theory may add a new perspective, but it does not render the panopticon irrelevant. The concept of 'disciplinary power' and the internalization of surveillance for behavioral control are shared by the two theories, Marx only never formalized it (Zuboff, 2015). Furthermore, Foucault's concept of 'disciplinary power' helps explain how workplace surveillance not only controls behavior but also generates data that further reinforce power structures. For example, Polzer's (2023) study on managers in over 100 different organizations using what they call 'people analytics' shows how some employees were promoted based on communication patterns, prior work procedures and collaboration statistics. Modern data collection from surveillance produces knowledge about employees that shapes worker subjectivity beyond simple productivity monitoring.

Foucault's theories were also accompanied by ideas of localized resistance and the possibility of subverting dominant power structures in ways that align more closely with contemporary forms of policymaking and privacy advocacy. Therefore, it's a more nuanced view of resistance than the revolutionary approach often associated with Marx. Compared to Marx, Foucault's emphasis on the role of discourse in shaping power relations is particularly relevant to the goals of this paper and allow for a more flexible analysis in my opinion. That said it is important to note that Foucault's and Marxist approaches are not mutually exclusive. However, there is little to no research conducted that productively combines insights from both to develop a more comprehensive analysis of workplace surveillance specifically.

Deleuze and Guattari (2006) also attempted to improve upon the panopticon by introducing the concepts of deterritorialization and reterritorialization. In their theories, traditional boundaries can be broken and rebuilt. This can be directly connected to the erosion of boundaries between work and personal life as surveillance extends into their personal time and activities. Other scholars like Parreno and Demeterio (2021) have also pointed out how Foucault had different aims when developing his theories. However, these works also fall victim to the same shortcomings as the ones I have already discussed.

In summary, Foucault's theories, though pioneering, have faced valid critiques, particularly regarding their applicability to contemporary digital surveillance. Haggerty and Ericson (2000), Deleuze and Guattari (1987), and Marx all provide interesting perspectives aiming to modernize the panopticon. However, despite these advancements, Foucault's emphasis on power relations and the potential for resistance through policy actions remains relevant. The panopticon, with its focus on disciplinary power and self-discipline, continues to offer valuable insights. As such, the subsequent case study will employ the panopticon as a foundational framework to analyze effective surveillance policies in the workplace.

2.4 Legal Frameworks

Both the United States (US) and the European Union (EU) offer two contrasting approaches to current regulation. As mentioned before, personal data has become the target of most digital monitoring systems. So, the focus of most policy frameworks around this topic is data protection laws and protection of right to privacy (Aloisi & Gramano, 2019; Ajunwa et al., 2017). The EU's General Data Protection Regulation (GDPR) is a robust starting point, requiring that personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. It broadly defines the law's applicability to any operation or algorithmic processing in the workplace "which is performed on personal data. . . whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (European Union, 2016a). Under the GDPR, employers must have legitimate legal basis for processing employees' personal data. This presents an impressive set of protections for employees in theory; however, the grounds for this legitimate basis are somewhat vague. Art. 6 mentions some of them may include consent given by the employee, protection of vital interests, or tasks performed for the benefit of the public. A reliance on consent from employees may be insufficient in the context of Foucault's theories. The power imbalance between employers and employees complicates the notion of “freely given” consent, as employees consent to data mining and surveillance not out of genuine agreement but as a means of avoiding potential negative consequences. Despite this, an opinion adopted in June of 2017 to the GDPR specifically focused on the impact of today’s surveillance technologies. It includes all scenarios “where there is an employment relationship, regardless of whether this relationship is based on an employment contract” (Article 29 Data Protection Working Party, 2017). This is incredibly beneficial to the “gig” economy studied by Rosenblat (2018), setting a wide range of principles to apply to current methods in surveillance. Even critics of the GDPR applaud its attempts to outline risks posed by new technology including “the recruitment process, employee screening, monitoring ICT usage in person and in remote settings, wearable devices. All for monitoring time, attendance, and performance” (Aloisi & Gramano, 2019). The GDPR exemplifies a robust and unified approach to data protection in the EU, but the regulatory landscape in the United States is a stark contrast.

In the US, workplace surveillance is governed by a patchwork of federal and state laws, which provide fewer comprehensive protections compared to the GDPR. US laws focus more on sector-specific and procedural protections as opposed to overarching privacy principles. The primary federal laws addressing workplace surveillance and employee privacy include the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA). These laws aim to protect electronic communications from unauthorized interception and access, but they provide significant exceptions for employers, especially when the monitoring is conducted for “legitimate business purposes” or when the “communications systems are company-owned” (Determann & Sprague, 2011). This renders the initial goals of the regulation very narrowly applicable. Alongside this, these laws also do not include other forms of personal data, as opposed to the GDPR which covers broadly all forms (Keane, 2018). In addition to these federal laws, state laws very significantly in their scope and enforcement. For example, California’s Invasion of Privacy Act (CIPA) requires consent from all parties before recording confidential communications, while Connecticut law mandates that employers notify employees of digital surveillance and banning monitoring for the purposes of employee health (California Invasion of Privacy Act, 1967). So, state level protections can offer additional safeguards, but there is too much inconsistency across states, resulting in a fragmented legal landscape that complicates employee protections. It’s clear that the EU’s legal framework is better suited for preventing the exploitation of employee monitoring. Where the GDPR enforces data minimization, mandating that personal data collected must be adequate, relevant, and limited to what is necessary (European Union, 2016b), the US has no broadly applicable data minimization rule in federal law. Where the GDPR provides explicit right to access, rectification, and removal of personal data by the employee, the US has no federal equivalent. And where the GDPR requires data controllers to demonstrate compliance with its principles and maintenance of records of processing activities, the US has no universal accountability principle (European Union, 2016c).

In conclusion, this literature review highlights that the application of algorithm-driven surveillance in the workplace, while informed by historical and theoretical frameworks like Foucault's Panopticon, also requires contemporary interpretations to fully grasp its implications. However, as we have seen, the Panopticon remains relevant in understanding the internalization of surveillance and self-discipline among employees. Moreover, the review of legal frameworks in both the European Union and the United States reveals significant differences in how employee data is protected. The GDPR provides a comprehensive and robust approach to data protection, aiming to balance the power dynamics between employers and employees. In contrast, the United States' fragmented legal landscape offers fewer protections, highlighting the need for more cohesive and extensive regulations. Ultimately, though the regulatory landscape in the United States is criticized for a narrower approach to privacy law, even the far-reaching data protection frameworks like the GDPR may struggle when attempting to give complete protections in today's world where data-driven surveillance greatly consolidates the power dynamics to the favor of the employer. This leads to the driving question of this paper: How well does the GDPR empower employees in the face of modern workplace surveillance?

3 Methodology

To garner a better understanding of how well the GDPR empowers employees with today's surveillance technology, this paper examines a variety of qualitative and quantitative data to conduct a literature review. I first explore two specific aspects of the GDPR relevant to modern workplace surveillance, breaking down the specific legal regulations and enforcement measures. Then, I evaluate the impact these specific regulations have had so far on workplace power dynamics, using Foucault's theories as a guide for determining if a disproportionate amount of power is held on the side of the employer.

The data used for this study is not collected by me; I am pulling on various qualitative studies and empirical studies on the GDPR and its impact that have been written since the legislation's inception in 2018, as well as aspects of theoretical framework I have already discussed in the initial literature review. Almost all the research I have consolidated were conducted in the European Union, as that is the only place the GDPR is legally binding. To find evidence of a shift in employee power, I look at existing case studies, specifically Amazon and H&M, surveys, and interviews of workers who were subject to excessive employee surveillance in the European Union at one point. I also pull from legal analyses of the legislation itself. I do pull from cases across multiple countries and thus multiple contexts both legal and cultural.

Plenty of literature exists analyzing or providing evidence for the GDPR's impact, but less so on its impact on workplace surveillance specifically. The main works used to understand it in this context are either seminal legal work on current workplace surveillance practices (Aloisi & Gramano, 2020; Abraha, 2023) or others that provide metrics such as compliance rates, changes in surveillance practices, and employee perceptions of privacy (Hanley & Hubbard, 2020; Bodie, 2023). However, my data also comes from some grey literature and internet press releases. I try and avoid using these sources as much as possible but some provided important context for the case studies.

Ideally, the aim is to examine workplace and legal environments prior to and after the implementation of the GDPR. However, this leads to one of the many limitations of my analysis. There is a strong reliance on secondary data sources, meaning the analysis is contingent on the availability and quality of existing literature and reports. Not only is there limited empirical research around the direct impact of the GDPR on workplace surveillance, weakening my conclusion, there may be gaps or biases in the existing data that could have affected my findings. For example, Hanley and Hubbard's (2020) look into Amazon's surveillance practices is a critical part of my review but their examples may have been selected based on their availability and prominence in public discourse, potentially leading to an overrepresentation of extreme cases of surveillance abuse and underrepresentation of more moderate or compliant practices. Using mostly secondary data sources introduces a level of dependency where my conclusions are influenced by prior sample selection and interpretation, potentially perpetuating any existing biases. It also may not capture the contextual nuances of specific cases. For example, the cultural and operational specifics of Amazon France Logistique or H&M might not be fully understood through secondary reports alone, making the analysis less nuanced.

My analysis also only incorporates relatively recent enforcement actions. This was necessary due to the lack of substantial reporting on other cases. However, this temporal limitation may not provide a long-term perspective on GDPR efficacy in shaping workplace power dynamics. My analysis of these cases is also then limited in that I am only selecting cases involving larger companies, weakening the applicability of my findings to smaller businesses also impacted by the regulations. The qualitative nature of my study means that the findings on the relationship between GDPR and power are mainly theoretical; therefore, interpretive, and as I mentioned not necessarily generalizable to all contexts. Future research on the topic would benefit from more quantitative methods for a more comprehensive assessment.

4 Applications: The GDPR in Practice

4.1 Proportionality and Necessity

The GDPR imposes stringent requirements for proportionality and necessity in processing personal data, particularly concerning workplace surveillance. Yet, this can often contribute little to empowering employees. Article 6 of the GDPR outlines the lawful bases for data processing, emphasizing that such actions must be strictly necessary for the specified purpose and not merely convenient. The Court of Justice of the European Union (CJEU) interprets this necessity narrowly, meaning employers must demonstrate that workplace monitoring is “essential to achieving a legitimate aim”, such as security or productivity, and that no less intrusive means are available (European Data Protection Supervisor (EDPS), 2024). Proportionality, however, a core EU law principle, demands balancing the means used against the intended aim. For workplace surveillance, this means the benefits must outweigh the privacy rights infringements, and only data that is adequate, relevant, and necessary should be collected. Employers must identify a lawful basis under Article 6 GDPR, often legitimate interests and conduct a Legitimate Interests Assessment alongside a mandatory Data Protection Impact Assessment for high-risk processing activities.

Transparency is crucial, requiring employers to inform employees about surveillance purposes and data processing. Appropriate safeguards, including limited scope and duration, restricted data access, and secure storage, are required to be implemented. The necessity and proportionality requirements significantly restrict blanket surveillance, necessitating employers to explore less intrusive alternatives, minimize data collection, justify special category data processing under Article 9, set data retention time limits, and regularly reassess surveillance justifications. All of this sounds ideal for tackling issues around workplace surveillance, but policymakers clearly opted for a principles-based approach rather than a rules-based approach. This is potentially to contend with the rapid pace of development for new surveillance technologies.

Kensbock and Stöckmann (2021) argue that many modern workplace structures trigger an intrinsically motivated process during which employees adopt a learning orientation, consequently motivating them to engage in what they describe as 'voice behavior', the voluntary communication of ideas, suggestions, or concerns by employees to improve organizational functioning. However, this beneficial process is counteracted by perceived surveillance via technology. When employees feel that a company structure is accompanied by increased surveillance, they are less likely to adopt a learning orientation and therefore less likely to engage in 'voice behavior' (Li, Li, Li, Zhang, & Li, 2023). The GDPR requirements in Art. 6 then make sense as not just a practical effort, but a group of policies that can theoretically be mechanisms to counterbalance the pervasive influence of Foucault's notions of power in today's workplace. By demanding that surveillance be necessary and proportionate, the GDPR curbs the potential for excessive monitoring and normalization, thereby protecting employees from undue control and categorization. This simultaneously applies to the constraints put upon the collection and processing of health and biometric data that ensures employees' bodies and lives are not subjected to disproportionate scrutiny and management. These specifications can create legal and ethical checks on employer power. Evidence from (Moorhead, 2020) indicates that employees who are less monitored are more likely to perceive surveillance as fair and legitimate, leading to increased job satisfaction and reduced stress. However, not all evidence is supportive of the strict 'proportionate' definitions under EU law as a method to build employee power. To maintain these requirements, the GDPR also necessitates extensive documentation and monitoring of data processing activities to ensure compliance. This could lead to a more detailed and systematic approach to surveillance, as organizations might implement more sophisticated tracking and monitoring systems. Findings by Siew and Boon (1998) reveal that tighter work monitoring can often accompany attempts at empowerment in a reengineered work environment. Their study on business process surveillance restrictions at the Singapore Internal Revenue Services showed that while it aimed to dismantle traditional hierarchies and increase employee autonomy, it often results in intensified monitoring and formalized behaviors.

4.2 Amazon France Logistique

The case of Amazon France Logistique brings to light significant concerns regarding the actual effectiveness of the GDPR to consolidate employee power. In December 2023, the French Data Protection Authority (CNIL) imposed a substantial fine of €32 million on Amazon's French logistics arm. This enforcement was caused by the company's use of an intrusive system for monitoring employees' activities and performance, as well as deploying a video surveillance system that lacked proper information safeguards. Specifically, the CNIL cited violations of the principles set forth in Art. 6 of the GDPR (European Union, 2016d).

Prior to the recent investigation, employees would enter the warehouse and were watched by the "extensive network of security cameras" (Hanley and Hubbard, 2020). This included "Distance Assistants", an algorithm-powered monitoring model attempting to maintain a certain distance between employees by measuring employee walking behavior (Hanley & Hubbard, 2020). Other modes of surveillance used were increasingly Orwellian. Employees wore biometric indicators that tracked how quickly items were scanned to determine working pace, flagging managers when some moved too slowly. Ultimately, the CNIL concluded that assisting or reassigning an employee does not require "every detail of the employee's quality and productivity indicators" collected using scanners and video footage (Walton, 2023). This is a near perfect reflection of the panoptic principles proposed by Foucault in the visibility and internalization of surveillance. Prior to enforcement of the GDPR, the employer dominated in their power with the ability to correct deviations from a norm Amazon established. We see evidence of this from descriptions of work conditions from employees themselves, who felt trapped in a constant state of observation:

"I have learnt to keep an extensive log of where I go and what I do in case I get asked why I've had a spike. Ultimately, we get on with it, but it's stressful having to constantly prove you are not making errors. Managers often lie about your rate and tell you that you're getting a lower rate so that you'll work faster... if you fall into the bottom 25, you'll be called for a meeting with management." (Hanley and Hubbard, 2020)

In essence, we have a situation very accurately aligning with Foucault's theories, and a set of principle-based laws designed with the intent to disable panoptic characteristics of the workplace. But practically, there were mixed results of the fine and enforcement of GDPR standards. Amazon stated they chose to disable the working pace scanners and extend time limits before inactivity indicators, which was a promising sign. But while these immediate changes stepped toward an improvement of the working conditions, they did not fundamentally alter the existing power dynamics at play. Largely, the surveillance system stayed intact. The core issue of surveillance to control remains largely unaddressed.

4.3 Exploitation and Enforcement Issues

The problem is that, despite definitions set by the GDPR, what constitutes a necessary or proportionate form of surveillance seems to be abused by employers. It is very context dependent across companies, industries, and business models. and can easily be argued that any employee monitoring is necessary for business purposes that the company defines themselves, similar to how an employer sets the norms of the employees through the surveillance. Automated and algorithm-powered surveillance tools are constantly innovating, creating new analytics and new ways to control behavior (). Along with this, data is an essential piece of nearly every major business in the world, incentivizing employers to monitor beyond what is just necessary. Because of this, businesses can easily blur what is employee data and what is business-related data (Bodie, 2023). In certain situations, employee data can be used to predict and halt the exercise of employee rights to protest and organize. In fact, Amazon France Logistique managers exerted control over their workers in this exact way. Warehouse cameras were served to disrupt workers' unions. As employees would gather, managers utilized surveillance tools and their "digital assistants" to break up groups and conversations, then refocusing individuals on work-related tasks (Hanley and Hubbard, 2020). Clearly, employers are likely to continue to deploy automated monitoring and decision-making technologies in ways that significantly harm workers' power without further guardrails.

The extent to which the fine served as punishment enough to mitigate future offenses is also questionable. In addition to the recent employee surveillance investigations, Amazon was already fined €746 million in 2021 by the Luxembourg National Commission for Data Protection (CNPD) after an investigation found some advertising practices were noncompliant with GDPR standards. That fine is still under appeal but signals a pattern of continued noncompliance. Historically, large companies have known to absorb fines as a business strategy, continuing the operations that gave them the fine regardless. This is especially true with corporations that generate substantial revenues like Amazon. In this case, the €32 million fine could be covered with just 32 minutes of daily income (Freedman, 2024). Another example, Apple was fined over €2 billion by the EU for violation of antitrust laws. However, this amount is less than two days' worth of company earnings, given its annual revenue of over €383 billion (Freedman, 2024). This is simply one aspect of a much larger array of issues related to the actual enforcement of the GDPR. While it provides the power to impose fines of up to 4% of company revenue, it does not provide the power to directly stall or end operations of any business. With limited enforcement measures, there are several challenges that limit the GDPR's effectiveness.

The main challenge to enforcement is resource disparities. Regulatory bodies often have less money and fewer resources compared to the large companies that are often the biggest offenders. As seen from Amazon, these companies can engage in prolonged legal battles, appealing to fines and sometimes succeeding in reducing them. The Wall Street Journal was subject to several fines in 2021, but 15 appeals were submitted for fine reductions within six months. In one of the appeals, a German court completed overturned a fine due to issues identifying the employee responsible for the violation (Heine, 2021). This contributes to a lack of uniformity in how the GDPR is enforced across different EU member states, leading to inconsistencies in penalties and compliance expectations. So, while enforcement is possible, there are still significant gaps in its effectiveness. In a survey of over 1,000 data protection professionals working in European companies, "74% say that authorities would find 'relevant violations' if they would walk through the door of an average company (?, ?). We see similar results in the GDPR's concept of consent.

4.4 Consent to Surveillance

The GDPR attempts to ensure that employees have clear control over their personal data. Just as anything collection of data or surveillance of work must be necessary and proportionate; it must also come with direct consent from the employee. Article 7 of the GDPR elucidates the nature of consent, stipulating that it must be a "clear affirmative act" (European Union, 2016b). This means that consent should be given freely, be specific, informed, and unequivocal. The recital emphasizes that this consent can be demonstrated through various forms such as written or electronic statements, or even oral declarations. People must be notified if they are being monitored. The essence of this requirement is to ensure that employees are fully aware of and agree to the surveillance in a manner that leaves no room for misinterpretation. Moreover, the burden of proof lies with the employer, who must be able to demonstrate that the employees have indeed given their consent. Recital 32 reinforces this requirement, underscoring the importance of transparency and accountability in data processing activities (European Union, 2016c). The ability to provide evidence of consent is crucial, as it fortifies the data subject's rights and the integrity of the consent mechanism within the GDPR framework. Further refining the concept, Recital 43 states that for consent to be valid, it must be "specific to each processing purpose" and should allow for "separate consent for different operations" (European Union, 2016d). It highlights that consent is not deemed freely given if it is bundled with other terms or if the provision of a service or contract is contingent upon consent for unnecessary data processing. However, as explained in WP29 Opinion 2/2017, "employees are seldom in a position to freely give, refuse or revoke consent" in an employment context.

The inherent power imbalances between employers and employees are why consent in the GDPR is so contentious. Some research has shown that the GDPR is effective in that employees are more willing to consent to surveillance with it in place. Surveys consolidated by Sekulovski (2023) provide evidence that the GDPR's disclosure requirements serve as an educational tool. When the employees of the companies surveyed understood what their data was used for, they were more likely to be okay with the surveillance. Vitak and Zimmer's (Vitak & Zimmer, 2021) work is less applicable for this purpose, as their research was conducted on US companies, but still provide insight into why employees consent to surveillance. Based on their empirical study, employees with a high level of trust in their management tend to perceive tangible benefits from surveillance, such as increased safety, easier task management, and reduced workload. However, those that do not trust management felt that consenting to surveillance was a trade-off for job security. Practically, it has been observed by regulatory authorities, policymakers, practitioners, and academic researchers that consent is typically insufficient legally in workplace settings (Crawford and Ajunwa, 2017). Abraha (2023) also proved that employees often worry that refusing to consent to surveillance could lead to unfavorable treatment in the workplace, such as being overlooked for promotions or facing job termination. This is another panoptic effect on display; employers utilize their positions of power to force compliance or provide employees with disciplinary consequences. Modern surveillance technologies equip employers with the information necessary to reinforce existing asymmetries between them and employees, leading to the argument that "consent alone should not be taken as the legal ground for an employer's surveillance of employees" (Hallinan, 2020). The GDPR's principle of consent is thus challenged in the employment context because the regulation does not adequately address the unique characteristics of employer-employee power. The lack of specific, binding rules for data protection in employment relations at the EU level exacerbates this issue, leading to varying degrees of protection and enforcement across different Member States. The result is a fragmented regulatory landscape where the protection of employee data depends heavily on national laws and collective agreements, which may not always align with the GDPR's objectives of ensuring free and informed consent. In some jurisdictions, like Portugal, there are explicit prohibitions against using consent as a legal basis for processing employee data if it results in an economic or legal advantage for the employee (Abraha, 2023). This reflects the understanding that such consent is not truly voluntary. However, in Germany, the reliance on general provisions under the Federal Data Protection Act (BDSG) for employee data protection has led to significant legal ambiguities and inconsistencies. The Hanover Administrative Court's decided to uphold Amazon Germany's real-time monitoring practices in the presence of proven consent, despite objections from the Lower Saxony Data Protection Commissioner (Abraha, 2023). This exemplifies the potential for misuse and overreach in the absence of clear, stringent rules. Recall from the literature review that this was the primary criticism of the United States legal framework.

4.5 H&M

In October 2020, H&M faced significant repercussions for violating the GDPR due to its illegal surveillance practices at the Nuremberg service center. The Hamburg Commissioner for Data Protection and Freedom of Information imposed a €35.3 million fine, highlighting severe breaches in employee privacy and data protection. This involved extensive and intrusive data collection on employees' private lives, including family issues, religious beliefs, health conditions, and vacation experiences (*Fine issued against HM for data protection violations*, 2020). This case underscores the difficulty of obtaining genuine consent in an employment setting, as employees are in a dependent position relative to their employer. H&M's surveillance practices involved collecting monitoring of personal data often without clear communication about the extent and purpose of the collection. Employees were likely unaware of how their data would be used, stored, or who would have access to it, making any purported consent neither informed nor specific (*H&M gets 35.3M euros fine for employees' personal data — GDPR Register*, 2020). Furthermore, consent needed to be freely given, meaning that there should be no pressure or negative consequences for withholding consent. The collected data was used for performance evaluations and creating detailed employee profiles, which could influence job security and career advancement. This context makes it difficult to argue that employees freely consented to the surveillance, as their refusal could have jeopardized their employment status.

Following the investigation, H&M implemented several measures including issuing an unreserved apology and providing financial compensation to affected employees, appointing a new data protection coordinator, and introducing monthly data protection status updates. The company also enhanced whistleblower protections and presented a comprehensive data protection concept to the Hamburg Data Protection Authority. Additionally, H&M committed to increased transparency regarding data collection and processing practices, ensuring future compliance with GDPR standards (*H&M gets 35.3M euros fine for employees' personal data — GDPR Register*, 2020).

This is another prime example illustrating both the limitations and potential strengths of the GDPR's ability to build employee power. The substantial fine and mandatory remedial measures underscore the GDPR's capacity to hold companies accountable and enforce data protection rights, thereby deterring future violations and promoting transparency.

However, the case also highlights significant challenges, such as the inherent power imbalance in employer-employee relationships that can undermine the validity of core concepts of the GDPR that enable surveillance to begin with. Compliance does not necessarily result in better workplace environments, as key provisions can be avoided almost entirely by morphing the interpretation of the exceptions. And the monitoring practices persisted for years before detection, indicating potential gaps in proactive enforcement. Between lackluster fines and loose restrictions on necessary surveillance, stronger legal protections are necessary for a more profound shift in employee power in the EU.

5 Discussion and Policy Reccomendations

Interestingly, initial conversations in the developing phase of the GDPR were a more promising starting point for combatting the rapid advance of surveillance technologies. The policy concerns and conversations in the European Commission were far more aligned with Foucault's theories, acknowledging that, in the future, almost "every behavior and practice in the workplace" had potential to be monitored and stored as data that employers could use to leverage power (European Data Protection Supervisor (EDPS), 2024). The huge risks to human dignity and foundational rights of employees were an importance. The commission tried to address this by welcoming comprehensive rules for the employer-employee dynamic as part of the final GDPR (European Commission, 2012). Specifically, three additions were considered: detailed rules on the interpretation of proportionality and necessity in the workplace context, further clarification on consent as a legal foundation for surveillance, and the introduction of a unique body to provide the ability to set specific rules for safeguards of data in the workplace. But ultimately, these additions were not implemented.

But because this more stringent rules-based regulations were not added, there are significant challenges to protecting employee power and the EU's legal landscape is fragmented and inconsistent in its enforcement and effectiveness of GDPR standards. For member states, it appears necessary that national legislation must align with overall GDPR objectives. Foucault's perspective would interpret this as a mechanism to prevent unchecked exercise of power by employers. But to be truly effective in protecting employee power, new national legislation must actively resist the normalization of surveillance by introducing distinct safeguards tailored to the employment context of that state. National rules should solidify protections, thus preventing employers from exploiting interpretations to expand surveillance. Based on the analysis, it seems that national rules must also include specific measures that safeguard human dignity, legitimate interests, and fundamental rights. This aligns with Foucault's emphasis on the importance of clear and enforceable limits to power. Specific safeguards help dismantle the implicit power structures that enable pervasive surveillance, ensuring employees have tangible protections. The following policy measures are recommended to practically implement these features and protect employee power and employee dignity. Specifically, these are to be additions or modifications to national level legislation of each member state of the EU.

5.1 Clarify Consent

National legislation must clarify the requirements for consent as a valid legal foundation. Consent, as we have seen, is often inappropriate in the workplace context due to inherent power imbalances between employees and employers. Opaque and sophisticated monitoring systems and new surveillance model algorithms further undermine this consent. The GDPR allows for states to create "specific rules ... for the conditions under which personal data in the employment context may be processed" (European Union, 2016c). This also includes the ability to prohibit consent as a means to process special categories of employee data. This new national legislation must clarify when consent is useable and identify contexts where it is not useable. For example, consent could be valid for processing associated with a legal or economic advantage for the worker but could be prohibited for algorithmic management systems in the workplace (Abraha, 2023; European Union, 2016d).

5.2 A More Stringent Proportionality

To properly regulate employee monitoring, the national legislation must balance between employers' legitimate interests and employee dignity and human rights, properly defining the GDPR's proportionality. Striking this balance is very important when the collection of employee data surpasses the requirements within contractual obligations of employers. Companies are often expected to perform this balance themselves, but it should not be entirely done by them. National legislation must create strict requirements that guide employers with enforceable rules. These rules should provide both employers and employees with the ability to access decisions that are allowed and not allowed. Set a clear boundary for proportionality using tests to determine what is appropriate in each context and where certain surveillance activities are entirely inadmissible. This proportionality test is possible to be derived from current legislative and regulatory tools, previous cases, and the existing GDPR principles. For example, the ECtHR's ruling in Bărbulescu v Romania outlines criteria for proportionate employee monitoring and WP29's Opinion 2/2017 creates guidelines for proper administration of novel technologies. Any new national legislation should codify these norms to create frameworks for measuring future compliance.

5.3 Scope of the Application

There are currently inconsistencies in GDPR principles by different states treating workers differently based on their legal status or the platform they work through, resulting in varied levels of protection and legal uncertainty. As an example, a proposed draft directive on platform work entirely excludes traditional employees, leading to discrepancies in protection (Del Castillo & Naranjo, 2022). To ensure fairness and uniformity, any new legislation on employee surveillance should not differentiate based on employment status; the protection of human dignity, legitimate interests, and fundamental rights should be universal for all workers, regardless of the legal nature of their employment relationship. Hence, the proposed legislation should apply equally to all types of workers, unless specific exceptions are stated clearly. This uniform data protection measures can enhance employee power by democratizing information control. By ensuring consistent data protection across all types of employment, the legislation would mitigate the power asymmetry between employers and workers, preventing employers from exploiting different legal statuses to impose varying degrees of surveillance and control onto different employees.

Article 88 of the GDPR provides a framework for regulating the purposes of employee surveillance by States. The phrase ”processing of personal data may be carried out in the context of an employment relationship” suggests that national rules should cover a broad range of data processing operations linked to employment relationships, not just those strictly required by the contractual employment relationship (European Union, 2016d).

Some case law supports a wide interpretation of Article 88, encompassing various surveillance methods associated with employment (CJEU, C-34/21 (n 4)63). Additionally, Article 88 acknowledges that workers have unique rights to dignity and privacy that general GDPR rules cannot entirely cover. Therefore, States need to focus on aspects such as transparency, data transfer within corporate groups, and workplace monitoring systems. Focusing on this would disrupt the traditional power dynamics in the workplace, fostering an environment where employees are more aware of their rights and the limits of employer surveillance.

5.4 Account for Algorithms

New surveillance technologies are equipped with machine-learning powered algorithms and are proliferating quickly. And according to Aloisi and Gramano (2019), "when it comes to designing a sustainable environment for data protection in times of [these systems], the GDPR may already be obsolete." The same directive on platform work previously mentioned has a solid starting point for States to regulate algorithmic surveillance. It gives specific rules to protect workers' personal data including restrictions on monitoring, collective employee rights, and transparency requirements (Del Castillo & Naranjo, 2022). This directive, however, focuses mostly on platform work, and states would need to extend its principles to all employees under algorithmic surveillance and data processing systems.

The Directive prevents processing personal data not necessary for contract performance and bans processing data on workers' emotional or psychological states, preventing an exercise of Foucault's biopower. These protections can be further detailed in new national data protection legislation. The Spanish Riders Law is another potential framework offering valuable inspiration for regulating algorithmic surveillance and can inform new legislation, requiring impact assessments for significant decisions and excludes consent as a legal foundation for algorithmic surveillance.

5.5 Improve Enforcement Measures

As the analysis showed, enforcement of the General Data Protection Regulation (GDPR) in the workplace faces challenges, particularly in the realm of surveillance. Authorities often struggle with resource constraints and lack of expertise, which hinders effective enforcement. To address these issues, there are several things for national legislation to consider regarding enforcement and institutions. First, establishing collaborative enforcement mechanisms between regulatory bodies is crucial. States should allocate responsibilities between authorities specifically in charge of data protection and labor authorities and mandate the exchange of information between them. Additionally, legally mandating trade unions and employee representatives to participate in the processes, as suggested by the German Advisory Council on Employee Data Protection, could help with capabilities of these entities (Gentile & Lynskey, 2022). Lastly, increasing the independence of data protection authorities within organizations could lead to more robust and unbiased enforcement of GDPR provisions.

6 Conclusion

Summary This dissertation has undertaken a comprehensive exploration of the complex dynamics surrounding modern workplace surveillance, with a particular emphasis on the implications of machine learning technologies and the GDPR on employee autonomy and employer authority. The findings reveal that the integration of digital surveillance systems, driven by sophisticated ML algorithms, has profoundly altered the ways in which employers monitor and manage their workforce. These systems extend beyond merely tracking productivity, encroaching into employees' personal lives through mechanisms such as health and fitness monitoring. This dual exercise of 'disciplinary power' and 'biopower,' as theorized by Foucault, illustrates the expansive reach of employer control in the contemporary workplace.

Implications The research highlights the significant reinforcement of employer power facilitated by digital surveillance technologies. These systems enable continuous, real-time monitoring with minimal human oversight, creating a self-perpetuating cycle where increased surveillance generates more data, thereby enhancing the predictive capabilities of algorithms and further entrenching employer control. This dynamic not only amplifies the power imbalance between employers and employees but also raises critical concerns regarding the autonomy of the workforce. The lack of transparency inherent in these technologies, coupled with the resulting self-regulation by employees, closely mirrors Foucault's concept of power being most effective when it is internalized by the subject. This phenomenon underscores the subtle yet pervasive ways in which digital surveillance can erode individual autonomy in the workplace.

While the GDPR aims to protect employees' privacy and autonomy by imposing stringent requirements on data processing, its effectiveness in addressing the power dynamics between employers and employees remains contentious. Although the regulation's principles of transparency, data minimization, and accountability are essential, their practical application often falls short in mitigating the evolving challenges posed by digital surveillance. This raises important questions about the adequacy of existing legal frameworks in safeguarding employee rights in the face of rapidly advancing surveillance technologies.

Future Research Looking ahead, there is a clear need for future research to focus on the development of more robust legal and policy frameworks that can better address the complexities of modern digital surveillance. This includes exploring ways to strengthen existing regulations like the GDPR to ensure they effectively limit employer power and protect employee rights. Additionally, interdisciplinary research that integrates Foucault's theories of power, Marxist surveillance theory, and contemporary data-centric approaches such as 'surveillant assemblage' could provide a more nuanced understanding of the multifaceted nature of workplace surveillance.

Another critical area for future investigation is evaluating the long-term impact of GDPR enforcement on workplace surveillance practices. This includes tracking changes in employer behavior and the extent to which regulatory fines and sanctions lead to sustained compliance. Specifically, quantitative research would be helpful to forming a more concrete conclusion, as most work on the subject is qualitative or theoretical. Insights from such research could play a crucial role in shaping workplace policies that prioritize both employee health and productivity in the digital age.

References

Abraha, H. H. (2023). Automated monitoring in the workplace and the search for a new legal framework: Lessons from germany and beyond. *Available at SSRN*.

Adey, P. (2006). *Deleuze and guattari (1987: 208). surveillance and security: Technological politics and power in everyday life*. Routledge.

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. *California Law Review*, *105*, 735.

Aloisi, A., & Gramano, E. (2019). Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the eu context. *Comparative Labor Law & Policy Journal*, *41*, 95.

Aloisi, A., & Gramano, E. (2020). Workers without workplaces and unions without unity: Non-standard forms of employment, platform work and collective bargaining. In *Employment relations for the 21st century* (p. 37-59).

Article 29 Data Protection Working Party. (2017). *Opinion 2/2017 on data processing at work* (Tech. Rep.). European Commission. Retrieved from `https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/201`

Ball, K. (2021). *Electronic monitoring and surveillance in the workplace* (Tech. Rep.). European Commission Joint Research Centre.

Bentham, J. (1962). *The works of jeremy bentham*. Russell & Russell.

Bodie, M. T. (2023). Employers as information fiduciaries. *Santa Clara Law Review*, *63*, 35.

Buchanan, B. (2020, August). *The ai triad and what it means for national security strategy* (Tech. Rep.). Center for Security and Emerging Technology.

California Invasion of Privacy Act. (1967). *California Invasion of Privacy Act, Cal. Penal Code §§ 630-638.*

Del Castillo, A. P., & Naranjo, D. (2022). *Regulating algorithmic management* (Tech. Rep.). ETUI, The European Trade Union Institute. Retrieved from `https://www.etui.org/publications/regulating-algorithmicmanagement`

Determann, L., & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in europe, destroyed in the united states. *Berkeley Technology Law Journal*, *26*, 979.

Ericson, R. V., Haggerty, K. D., & Murphy, C. (2000). Policing the risk society. *Canadian Journal of Sociology*, *25*(1), 111.

European Commission. (2012). *Staff working document sec(2012) 72 final* (Vol. 17; Tech. Rep.).

European Data Protection Supervisor (EDPS). (2024). *Edps investigation into the use of microsoft 365 by the european commission (case 2021-0518): Decision (8 march 2024)* (Tech. Rep.). European Data Protection Supervisor.

European Union. (2016a). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). *Official Journal of the European Union*, *L119*, 1-88. (Article 3-7)

European Union. (2016b). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). *Official Journal of the European Union*, *L119*, 1-88. (Article 9)

European Union. (2016c). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). *Official Journal of the European Union*, *L119*, 1-88. (Article 88)

European Union. (2016d). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). *Official Journal of the European Union*, *L119*, 1-88. (Recital 32)

Fine issued against hm for data protection violations. (2020). Retrieved from `https://www.simmons-simmons.com/en/publications/ckh3lyk2b14oj0917lz7sc9uf/fine-issued-`

Foucault, M. (1976). *The birth of the clinic.* Tavistock Publications Ltd.

Foucault, M. (1979). *Discipline and punish: The birth of the prison.* Vintage Books.

Foucault, M. (1980). The eye of power. In C. Gordon (Ed.), *Power/knowledge: Selected interviews and other writings (1972-1977)* (p. 146–165). Pantheon Books.

Foucault, M. (1985). Sexuality and solitude. In M. Blonsky (Ed.), *On signs: A semiotics reader* (p. 365–372). Blackwell.

Foucault, M. (2010). *The government of self and others: Lectures at the collège de france 1982-1983* (A. Davidson, Ed.). Palgrave Macmillan.

Freedman, R. (2024, May 13). *Big fines aren't burdensome for many companies, analysis finds.* Retrieved from `https://www.legaldive.com/news/big-fines-no-burden-for-companies-Tradingpedia-analysis`

Fuchs, C. (2013). Political economy and surveillance theory. *Critical Sociology*, *39*(5), 671-687.

Gandini, A. (2016). Digital work: Self-branding and social capital in the freelance knowledge economy. *Marketing Theory*, *16*(1), 123-141.

Gentile, G., & Lynskey, O. (2022). Deficient by design? the transnational enforcement of the gdpr. *International and Comparative Law Quarterly*, *71*, 799.

Hallinan, D. (2020). Broad consent under the gdpr: An optimistic perspective on a bright future. *Life Sciences, Society and Policy*, *16*(1), 1.

Hanley, D. A., & Hubbard, S. (2020). *Eyes everywhere: Amazon's surveillance infrastructure and revitalizing worker power* (Tech. Rep.). Open Markets Institute.

H&m gets 35.3m euros fine for employees' personal data — gdpr register. (2020). Retrieved from `https://www.gdprregister.eu/news/hm-gdpr-fine/`

Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review*, *44*(1), 161-175.

Keane, J. (2018). Application of data mining to "big data" acquired in audiology: Principles and potential. *Trends in Hearing*, *22*, 2331216518776817.

Kensbock, J. M., & Stöckmann, C. (2021). "big brother is watching you": Surveillance via technology undermines employees' learning and voice behavior during digital transformation. *Journal of Business Economics*, *91*(4), 565-594.

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2023). Mapping the empirical evidence of the gdpr (in-) effectiveness: A systematic review. *arXiv preprint arXiv:2310.16735*.

Manokha, I. (2020). The implications of digital employee monitoring and people analytics for power relations in the workplace. *Surveillance & Society*, *18*(4), 540-554.

Moore, P. V., Upchurch, M., & Whittaker, X. (2018). Humans and machines at work: Monitoring, surveillance and automation in contemporary capitalism. In *Monitoring,* *surveillance and automation in contemporary capitalism* (p. 1-16). Springer International Publishing.

Moorhead, B. (2020). An examination of support and development mechanisms for newly qualified social workers across the uk: Implications for australian social work. *Practice*, *32*(2), 145-159.

Moran, G. (2017). A recovery-oriented peer provider (ropp) work-role model and prototype measure. *American Journal of Psychiatric Rehabilitation*, *20*(4), 346-368.

Mulholland, K., & Stewart, P. (2014). Workers in food distribution: Global commodity chains and lean logistics. *New Political Economy*, *19*(4), 534-558.

Osterman Research, I. (2016). *Best practices for protecting your data when employees leave your company* (Tech. Rep.). Author Retrieved from `https://spanning.com/downloads/SBSU-whitepaper-osterman-protecting-data-when-employees`

Parreno, J. B., & Demeterio III, F. P. A. (2021). Metacritique on bentham and foucault's panoptic theories as analytic tools for three modes of digital surveillance. *Plaridel: A Philippine Journal of Communication, Media, and Society*, *18*, 1-48.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press.

Raval, N., & Dourish, P. (2016). Standing out from the crowd: Emotional labor, body labor, and temporal labor in ridesharing. In *Proceedings of the 19th acm conference on computer-supported cooperative work & social computing* (p. 97-107).

Rose, C. (2008). The challenges of employee-appointed board members for corporate governance: The danish evidence. *European Business Organization Law Review (EBOR, 9)(2)*, 215-235.

Rosenblat, A. (2018). *Uberland: How algorithms are rewriting the rules of work.* University of California Press.

Rosenblat, A., Kneese, T., & Boyd, D. (2014). Workplace surveillance. In *Open society foundations' future of work commissioned research papers.*

Sia, S. K., & Neo, B. S. (1998). Transforming the tax collector: Reengineering the inland revenue authority of singapore. *Journal of Organizational Change Management*, *11*(6), 496-514.

Silverman, B., Vogt, R., & Yanowitch, M. (2016). *Double shift: Transforming work in postsocialist and postindustrial societies.* Routledge.

Stanton, J. M., & Julian, A. L. (2002). The impact of electronic monitoring on quality and quantity of performance. *Computers in Human Behavior*, *18*(1), 85-101.

Vitak, J., & Zimmer, M. (2021). From watched at work to watched at home: Workplace surveillance during a pandemic. In *Aoir selected papers of internet research.*

Walton, A. (2023, March 7). *Amazon's surveillance culture is "breaking" its workers.* Retrieved from `https://www.huckmag.com/article/speaking-to-amazon-uk-workers-on-the-picket-lines-in-c`

Wood, D. M. (2016). Beyond the panopticon? foucault and surveillance studies. In *Space, knowledge and power* (p. 245-263). Routledge.

Zipperer, B., McNicholas, C., Poydock, M., Schneider, D., & Harknett, K. (2022). National survey of gig workers paints a picture of poor working conditions, low pay. *El Trimestre Económico*, *89*(356), 1199-1214.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.