Unregulated Surveillance Technology and Job Insecurity:

Necessity for Stricter Regulations in a Neoliberal Landscape

`

Jasmine Tajeddine
Student Number: 300230134

Major Research Paper

University of Ottawa
Faculty of Social Sciences
Graduate School of Public Administration

Supervisor: Professor Louis Simard

Table of Contents

List of Abbreviations

AI: Artificial Intelligence

CAP: Canada Assistance Plan

CHST: Canada Health and Social Transfers

CSE: Communications Security Establishment

CSIS: Canadian Security Intelligence Service

EI: Employment Insurance

FTC: Federal Trades Commission (U.S)

FTQ: Fédération des travailleurs et travailleuses du Québec (FTQ; Quebec Federation of Labour),

GDPR: General Data Protection Regulation

HDPA: Hellenic Data Protection Authority (Greece)

ICT: Information and Communications Technologies

IOT: Internet of Things

ISED: Innovation, Science, Economic Development Canada

OPC: Office of the Privacy Commissioner of Canada

PIPEDA: Personal Information Protection and Electronic Documents Act

RCMP: Royal Canadian Mount Police

List of figures

Acknowledgements

I would like to express my gratitude to my supervisor, Professor Louis Simard, for his patience, faith, and invaluable advice, and the Principal Academic Advisor, May Hamouie, for her guidance throughout this process. I also thank my friends and family for their support, with a particular mention Jeanine, Annie, and most especially, Theodore, as they have provided an unwavering support system throughout the entirety of my journey.

Abstract

With the enactment of Stay-At-Home orders due to Covid-19, labour markets have undergone a sudden shift to remote work. Despite many restrictions related to the pandemic being lifted, teleworking has persisted as a standard arrangement adopted by organizations, whether in a hybrid or exclusive manner. Regulatory measures specific to teleworking technologies remains a concern. Private sector organizations, in particular, have not been subject to regulation with respect to teleworking technologies. This paper conducts secondary research to explore the implications of a neoliberal governance paradigm through a Foucauldian lens and assesses Canada's Digital Charter with respect to the regulation of the private sector's utilization of digital and surveillance technologies. It compares these advancements with the teleworking guidelines framework established by Greece's Hellenic Data Protection Authority (HDPA). In doing so, the study demonstrates the impact of a neoliberal governance paradigm on Canada's Digital Charter through the absence of robust policy instruments necessary to establish correlation between the policies' objectives and their implementation.

Resumé

Avec la promulgation des ordres de rester à domicile, due à l'émergence de la Covid-19, les marchés du travail ont connu un changement soudain vers le télétravail. Malgré la levée de nombreuses restrictions liées à la pandémie, le télétravail s'est maintenu en tant qu'arrangement standard adopté par les organisations, que ce soit de manière hybride ou de manière totale. Les mesures règlementaires spécifiques aux technologies utilisées pour le télétravail restent problématiques. Les organisations du secteur privé, en particulier, n'ont pas été soumises à une régulation concernant les technologies de télétravail. Ce document effectue une recherche secondaire pour explorer les implications d'un paradigme de gouvernance néolibérale à travers une lentille foucaldienne et évalue la Charte numérique du Canada, concernant la régulation de l'utilisation des technologies numériques et de surveillance par le secteur privé. Il compare le progrès avec les directives du télétravail établi par l'autorité de protection des données hellénique en Grèce. Dans ce cadre, l'étude démontre l'impact d'un paradigme de gouvernance néoliberale sur la Charte numérique du Canada par l'absence d'instruments politique solides nécessaires pour établir une corrélation entre les objectifs des politiques et leur mise en œuvre.

Key words: Canadian Digital Charter, Foucauldian Analysis, Neoliberalism, Policy Implementation, Privacy and Security, Telework Technologies.

Introduction

Since the Covid-19 pandemic, telework has been amongst one of the leading factors of increased online activity. Teleworking has existed prior to the emergence of the pandemic, however, the use of remote work deviated from the standard, in-person working structure, and specifically granted individuals flexible work arrangements to accommodate personal circumstances (Pupo et al., 2012). In general, Covid-19 has played a significant role in accelerating digital transformation. With social distancing measures in place, digital technologies and tools were rapidly adopted and relied upon in diverse domains of life, spanning from retail to healthcare. However, the transformative shift it had imposed with regard to teleworking practices remains predominant, rendering what was once a non-standard form of employment, a new norm. The pandemic has accelerated the adoption of remote work, creating a sudden and more enduring change in the ways daily work is conducted. Organizations have come heavily reliant on digital communication tools, collaborative platforms, and video conferencing. With employees working remotely, employers, and their managers, have expressed that they question whether or not their employees are truly being productive (Tong, 2023). 85% of individuals in leadership roles have found that remote work has made it challenging to believe their employees are being productive (Microsoft WorkLab, 2023). The demand for employee monitoring software has increased by 75% in January 2022, and 54% in March 2023 since March 2020 (Migliano, 2023). There has been a 266% increase in searches with the phrase “best employee monitoring software” , a 125% increase in “employee monitoring software”, and 152% increase in “employee tracking software”, with software such as Hubstaff and Time Doctor gaining significant popularity (Migliano, 2023). Despite the fact that most Covid-19 related restrictions have been lifted, only 4% of individuals who adopted telework due to the pandemic have fully returned to in-person

work (Randstad, 2023). And, though the public sector has been standardized with its approach and tools to remote work (Carroll, 2022), this has not been the case for teleworking arrangements carried out in the private sector. With this, it becomes essential to take notice of the privacy and security implications of software features and functionalities used within organizations and the increased surveillance monitoring capabilities afforded to authoritative figures. Furthermore, this also renders it essential to assess the implementability of *Bill C-27*, Canada's recent Digital Charter, in regulating the matter with respect to both the socio-organizational and broader safety effects of the marginally restricted and non-regulated distribution and use of teleworking software. As Covid-19 had caused similar circumstances globally, in order to assess *Bill C-27* in Canada.

While telework, be it exclusively remote or hybrid, has led many people to feel more productive at work and with teleworking software being a tool allowing management to streamline, coordinate, and measure progress outside of the office space, Canada is in need of stricter and transparent regulations on surveillance technologies: Neoliberalism has led to significant levels of job precarity, and with increased monitoring and surveillance facilitated by teleworking tools, the asymmetrical power dynamic has intensified both the actual and perceived insecurity of jobs, indirectly pressuring many individuals to conform to the remote work arrangements chosen by their employers. The widespread adoption of telework has amplified online presence, causing a significant portion of society's digital footprint to expand involuntarily and, past a certain extent, unknowingly. Thus, the neoliberal governance paradigm facilitates the distribution, use, and exploitation of surveillance technologies, resulting in heightened power imbalances within workplaces, and thus rendering cautious and voluntary online activity increasingly difficult to undertake.

In order to assess the implementability of Canada's recent advancements in its Digital Charter, this research paper will begin by carrying out an in-depth review of relevant literature related to the subject matter, encompassing academic articles, studies, and other academic sources that will serve to provide insight, in addition to theoretical frameworks pertaining to the topic at hand. The literature presented aims to establish a foundation of knowledge that will facilitate the development of this current research. Following the literature review, the theoretical approach presented aims to situate and frame the search topic with the Foucauldian theories of power, both disciplinary and security, in the context of public administration and governance. Guided by the chosen theoretical approach, the methodology makes use of a multi-case study and cross-sectional analysis for a comparative approach to assessing the legal decisions undertaken with respect to digitalization in Canada and in Greece. This chapter outlines the use of both documentary and archival information, the methods employed to gather relevant data, collection techniques, and the tools utilized to do so. With this information, chapter four aims to provide a comprehensive depiction of the present state of the teleworking environment in Canada and Greece, and the current state of its governance, including key events, and legal decisions taken to address the issue of digitalization and the future of work. With the description of both cases, chapter five serves to discuss and set a foundation to identifying gaps in implementability, procedures, and to explore potential solutions.

Chapter One: Literature Review

This literature review examines several subtopics to identify the current state of knowledge, and thus provide background information and a relevant theoretical framework. This chapter provides an overview of the ideological framework of neoliberalism and macroeconomics and its overt and covert implications on labour market policies and conditions of work. Moreover, it reviews literature pertaining to the use of technology under the neoliberal paradigm. Surveillance and monitoring literature serves to provide background on Foucault's contributions to panoptic surveillance and how this has been linked to surveillance technologies and the intensification of power imbalances. Through this lens, the intensification of surveillance, under a neoliberal economic paradigm, serves to enforce disciplinary power over employees to ensure and maintain productivity. Concerns related to surveillance technologies and telework have also been reviewed to recognize and acknowledge previously expressed apprehensions on this topic. Lastly, this chapter also attempts to highlight the current teleworking conditions by identifying the most commonly used software programs, their panoptic qualities. Together, these provide an overview of the core aspects related to the topic at hand and serves to establish a comprehensive foundation to position and contextualize the approach undertaken in this study.

1.1 The Implications of Neoliberalism on Labour Market Policies.

The neoliberal ideological framework, and thus its inherent economic policies, have significantly impacted labour market policies. The emergence of neoliberalism, as an ideological paradigm, has had a pronounced impact on both federal and provincial public policy and administration (Gill, 2021). Neoliberal governmentality holds the belief that state regulation of the labour market and guaranteed social protection serve as obstacles to economic growth (Clark, 2002).

Around the late 1970s, the political discourse pressured the country to adhere to neoliberal ideologies, such as international competition and reduction in the welfare state, and thus initiate reforms (Gill, 2021; Pupo et al., 2017). The de-industrialization of Canada occurring in the 1970s led to a great reduction in manufacturing employment, thus, in turn, expanding the service sector of the Canadian economy, where unionization rates plummeted (Pupo et al., 2017). Reliance on market forces played a central role in policy-related decision-making, as most policy developments were rooted in economic restructuring (Pupo et al., 2017). Within the neoliberal framework, the approach to policy innovation was central to the MacDonald Royal Commission Economic Union and Development Prospects for Canada in the 1980s, which succeeded greatly in carrying out policy reforms (Clark, 2002). Changes and reduction of social program funding, such as Employment Insurance (EI) had thus begun to occur (Pupo et al., 2017), and, in 1996, the Federal EI Act called for a federal and provincial government collaboration regarding labour market administration and led to federal/provincial bi-partite agreements (MacKinnon, 2011). Other significant changes made by the deferral government in social policy, such as the establishment of the Canada Health and Social Transfer (CHST) in 1996, mainly serving as a replacement to the Canada Assistance Plan (CAP), established in 1966 (MacKinnon, 2011). The CHST would relieve the federal government of sharing the costs of social spending, thus transferring greater responsibility for social assistance over to provincial governments (MacKinnon, 2011). Provincial governments have largely adopted neoliberal governmentality. The expansion of federal devolution of policy-related responsibilities enabled many provincial labour and social policy-making to adhere to neoliberal norms, in turn emphasizing social and labour-market flexibility (McBride and McNutt, 2007). As such, social security measures were largely replaced by labour market policies centered around skill development and competition.

These policies aimed to achieve policy objectives related to increasing employment rates (Kennedy, 2016).

1.1.1 The Implications of Neoliberalism on Framing Working Conditions.

The heavy emphasis placed on a market-based policy framework enabled non-standard forms of employment, such as telecommuting/telework, or flex-work, to bourgeon, consequently eroding labour rights and employment protection (Manokha, 2020), ultimately increasing insecurity and precarious employment (Pupo et al., 2017). Cuts made to social spending and policy, erosion of the social safety net, alongside the competitive principles of neoliberal rationality, have amounted to increasingly precarious jobs (Gill, 2021). Governments have long acknowledged that service sector work holds the lowest rates of unionization and the highest rates of monitoring (See U.S. Congress, Office of Technology Assessment, 1987). Macroeconomic trends associated with neoliberalism brought increasingly competitive markets and pressured employers to operate with as minimal costs as possible (Pupo et al., 2017). As such, monitoring became a central mechanism in ensuring that labour is as productive and cost-effective as can be. The repercussions of deregulation have rendered the job market highly competitive, in which employers search for cost savings, and therefore productivity (Pupo and Duffy, 2012). The growing power imbalance as a result of the reduction of social safety alongside the emphasis on productivity has been shown to amount to the exploitation of compliance (Pupo and Duffy, 2012). Moreover, in addition to compliance, in the light of an increasingly precarious job market, it is often indirectly required for workers to be wary of behaviour and maintain reputability (Jackson and Thomas, 2017; Pupo and Duffy, 2012). The impact of neoliberalism has led to what

has been described as “liquid modernity”, as working conditions under neoliberal ideologies are characterized by instability and vulnerability (Gane, 2001).

1.1.2 Neoliberalism and Technology.

The neoliberal paradigm played a significant role in the shaping of the Internet that should not go overlooked. It was not until the 1980s that the Internet began to expand and not until the early-mid 90s that the Internet was commercially accessible to the public (Leiner et al., 1997). In the late 90s, telecommuting began to popularize as teleworking was perceived to have significant benefits, including increased productivity amongst employees (Shore, 1999). The Internet, and concurrently digital aspects of remote work and digital distribution programs, was largely influenced by the greater paradigm in which it emerged. Internet governance was set out to be free from government regulation and characterized by competition and bottom-up regulation (Chenou, 2014). For this reason, the widespread adoption of the Internet under the neoliberal paradigm is important to consider. The political and economic conditions enabled the surveillance advertising industry to grow rampantly (Crain, 2021). Continuous increase in profit margins lies central to the practices of neoliberalism, and thus, the Internet, and its technical by-products are widely used accordingly (Fenton, 2011).

As such, by the 1990s, surveillance had become an inherent feature of the web and digital distribution platforms (Crain, 2021). Struggles to reform Internet governance due to surveillance concerns, especially under neoliberal governmentality, have been discussed within the American literature. In 1996, privacy activists urged the U.S Federal Trades Commission (FTC) to establish federal regulation on digital surveillance operations (Crain, 2021). Nonetheless, the FTC agreed with industry arguments and declared that industry self-regulation was the

preeminent method to address concerns of privacy, ultimately overlooking establishing guidelines (Crain, 2021). Though Canadian literature on neoliberal implications on the Internet is scarce, neoliberal governmentality and its approach to Internet governance remains pertinent. The monitoring of behavior through Internet usage has been steadily increasing, as the neoliberal reduction of government regulation and oversight has significantly facilitated the proliferation of private surveillance companies (Zureik, 2020).

1.2 Surveillance and Monitoring

As teleworking became increasingly available along with technological advancements, the area of research began to expand. Michel Foucault's (1975) contribution to the overarching theme of surveillance, through concepts of social regulation, disciplinary power and panoptic surveillance, has been central in discourses pertaining to teleworking. The topic of workplace surveillance primarily began to popularize alongside the rise of the neoliberal paradigm (See U.S. Congress, Office of Technology Assessment, 1987). Workplace surveillance raises privacy, ethics, and human rights issues (Ball, 2010). Surveillance and monitoring have been discussed in an array of concepts relating to privacy, such as privacy pertaining to social relations, personal space, and information privacy (Ball, 2010). From a Marxist perspective, digital labour under a neoliberal economy introduces a new avenue for the expansion of power imbalances. Granted the social conditions emergent from neoliberalism and social powers of those with managerial-type positions in the workplace, digital production of labour has the opportunity to provide individuals who occupy managerial roles with private power (Marx, 1894/1981 as cited in Fuchs, 2019). On this note, a recent Canadian report has indicated that a large majority of teleworkers remain uncertain about what monitoring software are precisely observing (Anaya, 2022).

The medium between power and control, today, is largely attributed to the use of surveillance, and thus the data an individual generates through the data produced (Fuchs, 2019). Working in cyberspace enables a digital panoptic mechanism, and thus a digital dimension of power (Manokha 2018). Digitalization does not solely offer a different avenue for control but facilitates its intensification as it broadens the scope of surveillance (Graham and Wood, 2003). Early studies of teleworking have indicated that individuals with weaker relationships with their managers are affected by the intensification of control. Despite that managers are certainly required to monitor employees to a reasonable degree, technology provides authoritative figures with information that they would have not originally requested (Lally, 1996). Studies have also shown that organizational monitoring, such as monitoring attitude, behaviour, efficiency, quality, and quantity of tasks assigned to the individual, increases organizational power, particularly during recessions and economic decline (Taekke, 2011). Performance, primarily during economic downturns, is crucial to the employment status of the individual. Organizational monitoring can be used as a coercive tool, increasingly appropriated to exploit compliance (Taekke, 2011) as workers have expressed that they feel pressured to accept surveillance and monitoring should it be at the expense of employment (Delfanti and Frey, 2020). This has left researchers wondering how the implication of surveillance is and will continue to shape the conditions of work for future generations to come, and how these workers are to resist and negotiate surveillance and monitoring altogether (Ball, 2010).

The exploitation of surveillance and monitoring is not unique to the private-sector and coercive managerial practices. Extensive surveillance and monitoring can be identified on a larger, governmental scale. Government-grade spyware, such as Pegasus spyware, a program

developed by a privately held Israeli technology firm, is sold by the NSO[1] Group to vetted governments (Chawla, 2021). The considerable growth of surveillance technologies alongside the political and economic neoliberal transition is largely associated with the deregulation and privatization of the state (Zureik, 2020). In addition, with technology increasingly becoming indispensable to quotidian life, government agencies have had increasing interests and inclinations towards digital surveillance (Deibert, 2022; Zureik, 2020). The NSO group is one of several upscale companies in the ever-growing surveillance technology marketplace, whose targeted clientage consist of mainly governments and government agencies (Deibert, 2022). Other companies include Gamma Group, an anglo-german company headquartered in Italy, and Cytrox, based in Skopje, Macedonia. The upper-scale surveillance technology industry markets its programs and capabilities to governments by presenting their services as tools to investigate serious crime (Deibert, 2022). However, without government regulation, such products can be (and have been) misused to undermine political accountability and overpower political opposition (Deibert, 2022).

1.2.1 Current and Prior Concerns

The Internet can be seen as the by-product of and the key instrument in the recent political economy (Schiller, 1999). As such, concerns regarding the intensification of monitoring and surveillance through telework have been present prior to the emergence of Covid-19. Studies have highlighted the implications of the political economy, and the ways it has increased coercive measures and power imbalances in the workplace due to precarious conditions and

[1] NSO stands for Niv Karmi, Shalev Hulio, and Omri Lavie, names of the individuals who founded the group in 2010 (Kaster and Ensign, 2023).

compulsory compliance (Pupo and Duffy, 2012). Surveillance has been a tool to ensure the utmost productivity among workers in physical workplace environments, however, the digitalization of a workplace environment facilitates surveillance and monitoring of subordinate employees, thereby further polarizing power between subordinate and authoritative actors (Manokha, 2018). The digitalization of a workplace increases an organization's panoptic properties (Manokha, 2018), as technologies used to carry out monitoring have been found to make employees feel powerless and vulnerable (George, 1996). In a fragile era for job retention, which already grapples with union organizations, digital worker surveillance further impedes collective action and poses great challenges in attempts to unionize (Garden, 2018).

As demonstrated, concerns over the power imbalance between employer and employee occurred prior to the pandemic, however, post-pandemic discourse over unjust power relationships in teleworking has been considerably pertinent (Allen and Masters, 2021; Clary, 2022; Sládek and Sigmund, 2022). Moreover, decision-making reliant on AI-generated statistics has broadened the discourse on teleworking and the nature of employment relationships. The growth in technological accessibility, consequentially rendering telework accommodations increasingly attainable, had begun to transform employment relationships and thus leading to questions about the suitability of labour policies given the increasing rate of remote work (Lowe, 2002; Trudeau, 2002). The pandemic has played a significant role in reshaping what consists of 'standard' forms of work. Along with the pandemic's push to the widespread adoption of teleworking arrangements, there has been a sizeable expansion of tools developed to carry out digital monitoring to ensure productivity among employees (Aloisi and De Stefano, 2022). The expansion and intensification of productivity-safeguarding mechanisms have brought forth major privacy concerns and the consequences of a data-collecting technology as a method of

supervision, as opposed to traditional managerial supervision (Bérastégui, 2021). Though there have been calls made to modernize policy prior to the telework eruption in 2020, some have argued the necessity for a new paradigm for labour policy due to its incapacity to account for transformations in employment relationships (Lowe, 2002; Trudeau, 2002) and others arguing that the law of employment surveillance designed for the physical world is ultimately unfit for the digital world (Garden, 2018), the large-scale adoption of this form of work calls forth policymakers to address the gradual diminution of a physical workplace environment (Bérastégui, 2021; Abulibdeh, 2020). Teleworking schemes were put in place at the beginning of the pandemic, however, such policies are limited and should remain temporary, as they were solely assessed in the scope of risk and thus only within the context of Covid-19 (Abulibdeh, 2020).

The digitalization of work and the progression toward algorithmic management were also called to attention prior to the pandemic (Adams-Prassl, 2019; King and Mrkonich, 2016). Concerns over the performance monitoring and A-I-driven decision-making progressively seeping its way into an integral aspect of managerial functions under contemporary legal regulation of employment were argued to be problematic, particularly due to the elimination of human discretion (Adams-Prassl, 2019; Graham and Wood, 2003). Early research attempted to disprove the proposition that technology is a neutral tool and highlighted the socio-political consequences of policy making under this assumption (Henman, 1997). Recent discourse has thus begun to account for the implications of AI-generated data collection and how it may contribute to workplace discrimination (Allen and Masters, 2021; Noble, 2018; Gal et al.,). For instance, candidates considered for job opportunities within an organization may be selected on the basis of reliability or flexibility, using data inputs to assess the employees most active during

the busiest times (Allen and Masters, 2021). In such a scenario, in which AI-generated data is used for decision-making, women, for instance, could be placed at a disadvantage due to disproportionate caring responsibilities, as data inputs are purely statistical and thus do not consider the reasons for absence or limited flexibility (Allen and Masters, 2021). Artificial Intelligence (AI) and analytics software founded on collecting employee data for reasons of assessments or decisions has become increasingly popular with the market for such technology having an estimated growth from 1.1 billion in 2018 to 2.2 billion by 2023 (Masoodi et al., 2021). There is a growing apprehension regarding the impact of AI and its progress towards displacing lower-skilled workers from their jobs, in addition to concern that this displacement will extend to advanced fields in the near future (Thormundsson, 2023).

Moreover, it is important to note how the involuntary adoption of telework, emerging due to the Covid-19 pandemic, has significantly increased online engagement and activity due to teleworking and videoconferencing (Mouratidis and Papagiannakis, 2021). With involuntary increased online activity, the expansion of one's digital footprint, and the erosion of boundaries between work and home (Haider and Anwar, 2023) has led to greater emphasis placed on taking appropriate precautions (Shaw, 2022). Malware may also include spyware, which may be defined to work "…by installing itself on a device without someone's consent or providing adequate notice. Once installed, it can monitor online behavior, collect sensitive information, change device settings, and decrease device performance" (Microsoft Security, pp. 8, 2023). The installation of spyware can be facilitated through phishing attacks, which have experienced a noteworthy surge in prevalence (Petrosyan, 2022). Instances of spyware, on a larger scale, have recently come to light. Within the public sector, government agencies have the resources to install "zero-click" spyware on devices, i.e., installation of spyware without the use of phishing

schemes. The Royal Canadian Mounted Police (RCMP) disclosed that it covertly uses spyware to conduct surveillance through the infiltration of devices in order to collect data, including the remote activation of cameras (House of Commons Canada, 2022). The House of Commons Access to Information, Privacy, and Ethics Committee initiated an investigation into the use of spyware by the RCMP. Concerns were raised regarding the use of spyware and violation of Canadians' right to privacy. However, according to the Canadian minister of Public Safety, Marco Mendicino, the use of spyware was only used to target serious offenses (House of Commons Canada, 2022). Nonetheless, expert and researcher on national security and intelligence, Michel Juneau-Katsuya, confirmed that it is highly likely that other government agencies, such as the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), employ technology similar to that of Pegasus (House of Commons Canada, 2022). In Greece's case, the country has faced allegations of engaging in the targeted surveillance of journalists and opposition politicians using spyware that hacks into their devices, with politicians from various European countries allegedly falling victim to attacks for political-gain driven objectives (European Parliament, 2023).

In consideration of the distinct yet pertinent circumstances, the perspectives on spyware and approaches differed between the two countries. As a response to the alleged misconduct, the Greek government announced its intention to ban the purchase of spyware (EU Reporter Correspondent, 2022). Greece's Ministry of Justice (2022) carried out a public consultation on the draft law, titled "Communications Deprivation Procedure, Cybersecurity and Protection of Citizens' Personal Data" in November of 2022. In Canada's case, the House of Commons' report on Access to Information, Privacy and Ethics concluded the need to further regulate spyware and other investigative tools of its nature, highlighting that as technological advances persist, so too

must Canadian law (House of Commons Canada, 2022). Recommendations as a result of deliberations included the creation of a banned list of spyware vendors, and a general the establishment of clear rules on the use and export of surveillance technologies. Additionally, suggestions included establishing privacy as a fundamental right, and that this be added to the Personal Information Protection and Electronic Documents Act (PIPEDA) (House of Commons Canada, 2022). In deliberation period, Ronald James Deibert, a Canadian professor of Political Science and the Director of the Citizen Lab based at the Munk School of Global Affairs and Public Policy at the University of Toronto, highlighted that in addition to the larger spyware issues within government operations, the surveillance technology industry invests substantial funds to identify software vulnerabilities and deliberately refrain from them in order to provide malware as a service through the sale of certain software (House of Commons Canada, 2022). However, no substantial action has been taken by the Government of Canada at the time of writing.

Since the involuntary adoption of telework, Canada's telework-force constitutes 40% of Canadians, in comparison to 12% prior to Covid-19 (Haider and Anwar, 2023). The recent surge in telework has resulted in significant increase of Internet use, resulting in higher levels of data being transferred (Sapenta and O'Brien, 2023). According to Statistics Canada's recent dataset on Information and Communication Technologies used by Industry and Size of Enterprises (2022), a significant proportion of companies in the private sector, specifically 49.4%, are operating software programs that are not specific to the companies' industry. 45.3% use cloud-based computing services, including (but not limited to) cloud-based software, cloud-based

processing power[2], and a cloud-based environment for application development and/or testing. Moreover, 22.2% of private sector employees are aware that their company uses a (or multiple) Internet of Things (IoT)[3]. Only 0.8% of private sector enterprises surveyed did not use the Internet to carry out business due to privacy and/or security concerns. This data is particularly interesting when considering data provided by the OPC's Departmental Plans and Departmental Results Report (2022): Results indicated that one in five Canadians have rated their knowledge of privacy rights as "poor" or "very poor", while 64% of those surveyed rated their knowledge to be moderate. Within the scope of privacy compliance, there was a general 5% decrease in OPC recommendations accepted and implemented by federal or private-sector institutions. However, the report shows that despite a reduction of accepted recommendations on the whole, private-sector institutions accepted fewer recommendations, regardless of the nature of the complaint relating to privacy rights. In comparison to results from previous years (2016, 2018), the OPC notes that despite significant technological advancements, the awareness of privacy rights amongst people has remained stagnant, with no significant changes in proportion. In the same report, 52% of private sector organizations rated their level of awareness of their responsibility under Canada's privacy laws as either "aware" or "extremely aware", while only 39% said their businesses provide their employees with privacy training or education.

Also recently reported, a lack of technological competence amongst teleworkers due to their poor understanding of security, such as misunderstanding of the functions of their Virtual

[2] Cloud Processing Power enables a company or business to carry out automatic and frequent data backups, storing data on multiple servers in multiple geographic locations (Leonidas, 2022).

[3] IoTs are defined as Internet enabled devices that use embedded systems, to collect, distribute, or act upon data that is acquired from their environments. IoTs may also be used to distribute and act upon data that collected by other IoTs (Gillis, 2022)

Private Networks and defaulting in creating best practices based on their personal interpretation of security and privacy (Obada-Obieh, 2022). Respondents received little to no guidelines on teleworking. Additionally, the findings indicated that workers felt obligated to compromise and overlook their privacy concerns to avoid facing potential professional drawbacks in their place of work (Obada-Obieh, 2022). The findings highlight the tension between professionalism and privacy on video calls, employees sharing their personal information to facilitate teleworking, the use of software programs to monitor activity, and the human and organizational dimensions of operating through technological instruments. Concerns revolved around the misuse and unauthorized sharing of shared personal data, loss of privacy, and accidental disclosure of information. Employees have expressed angst in relation to the monitoring of activities through the instruments used by management to carry out telework (Obada-Obieh, 2022). With software indicating the presence and status of employees, such as green icons symbolizing availability and active use of the computer, red symbolizing the user is occupied yet still actively on their computer, and yellow representing that the computer and/or software has been idle for a certain amount of time, workers have spent time worrying about the display of their availability status on the communication software. For instance, "... [Managers] might jump to conclusions [in] thinking that an employee should be either green or red, but not yellow because yellow means that they're [not] at the computer" (Obada-Obieh, 2022, p. 47). Angst surrounding professional reputability through demonstrating active presence within the digital workplace has been additionally highlighted in the use of video calls. The use of video-conferencing has been found to be quite prevalent in daily routine (Obada-Obieh, 2022; Labrecque et al., 2022). A recent study has indicated that video conferencing is used as a tool to make teleworkers feel less

isolated (Lebrecque et al., 2022). As such, remote workers have reported almost daily videoconference meetings with management to touch base and discuss daily plans. As teleworking software varies, not all applications used to carry out videoconferencing offer virtual or blurring-effect backgrounds, and even so, the background-altering technology might not be as stable as needed, thus unable to thoroughly guarantee that sudden movements made by the person on the videoconference will not trigger the application to accidentally display what is behind them. This instability may also be triggered by movements made by other people (or pets) behind the person in the video call (Obada-Obieh, 2022). Some have expressed discomfort in videoconferencing, as "you're inviting a lot of people into [your] home that [you] wouldn't have otherwise. So you're here [on the video call], your kids are walking by, or other family members or your dog or whatever the case may be, [and] you may not want people to see [all of that]" (Obada-Obieh, 2022, p. 45). Moreover, it has also been reported that it is common for noises or conversations made by others residing in the household to be captured on the microphone during a call. (Obada-Obieh, 2022).

In regard to misuse and/or unauthorized sharing of personal data, teleworkers have expressed angst in regard to employers accessing parts of their computers remotely. Privacy and security concerns are greatly related to the fact that employers, administrators, or any person granted authority and/or permissions, may access all information stored in one's computer, resulting in a great power imbalance (Obada-Obieh, 2022). The misuse of technology in organizational relationships has been found to be a prominent cause of actual or perceived power imbalances. The use of personal equipment when working from home has made teleworkers feel obligated to answer to calls that they would have not typically answered or emails on their

personal computers with links that they would have not wanted to interact with (Obada-Obieh, 2022). Teleworkers have voiced difficulties in discerning fraudulent phone scams or spear phishing emails and apprehension in declining calls from unfamiliar numbers due to concerns that their employers might become frustrated with any perceived decrease in productivity in the case the calls were legitimate (Obada-Obieh, 2022). In this regard, a study has revealed that individuals with low self-confidence in detecting phishing emails are less likely to report perceived illegitimate sources, due to fear of negative outcomes embarrassment or other negative socio-organizational outcomes (Kwak et al., 2020). In that respect, in a recent study, results of a questionnaire have indicated that employees who experience less technological issues are perceived to have greater levels of productivity (Catană et al., 2022). In a simulated phishing test, results showed that 20.3% of the target population had clicked on the suspicious link, while only 7.4% of people reported the phishing email (Kwak et al., 2020). Additionally, according to a recent global survey of working adults and IT professionals, it was found that 85% of cyber incidents experienced by organizations were phishing attacks (Petrosyan, 2022).

Moreover, technology has led to a significant intensification of power imbalances as employers have shown increased reliance on AI for hiring and subjecting their subordinate colleagues to increased surveillance (Yang and Liu, 2021). Here, it is important to note the impact of intersectionality when discussing the intensification of power imbalances among employers and subordinates. Though this is not the focus of this study, this paper acknowledges that women, ethnic minority groups, and LGBTQIA2S+ peoples may fall victim to additional systemic discrimination due to the increased systematic and technological advantages by their employers and are therefore likely to be disproportionately impacted by the implications of

monitoring and surveillance (Yang and Liu, 2021). As such, AI systems possess the capability to make decisions that hold considerable ramifications. With private firms developing AI programs, this often results in a lack of transparency with respect to their functionality, rendering equity, accountability, and safety difficult to assess (Thormundsson, 2023).

1.2.1.1 Current Tools Used in Canada

The global demand for surveillance-based technologies by employers has increased by 87% (Masoodi et al., 2021). The Microsoft Team application is used to empower all Canadian government employees in the public sector (Carroll, 2022). However, private sector employees have not been met with the same consistency upon shifting to remote or hybrid work. Communication platform software utilized to carry out telework in Canada's private sector varies. For example, Zoom, Skype, Microsoft Teams, Slack, Rainbow, Asana, and Discord, are typically utilized to facilitate collaboration between colleagues. These tools facilitate the establishment of a common space in the digital working environment and reinstate an archetypal workplace arrangement. They are used by organizations to enable colleagues to carry out video conferences or teleconferences for meetings or work-related conversations, create chat rooms, check one another's availability, and overall grant a medium for interaction and collaboration. They also often serve to facilitate team management, by project planning, task management, and overseeing workflow. These types of software typically also allow monitoring or productivity to a degree. For example, Skype has the capacity to generate a usage report to an administrator, by providing a "detailed activity of your members' Skype usage. This includes the time, date, duration and destination number of all calls and texts made and details of purchases and

downloads" (Skype website, 2023), whereas a software like Asana provides universal reporting, enabling one to “see and track work from every angle” and “get real-time insight into the state of your team’s work…” (Asana website, 2023).

Other software, such as analytics software, may be used independently or in addition to communication platforms. According to the “Employee Monitoring Software” page on Capterra’s website (n.d), a leading software review and selection platform, most reviewed software by Canadian companies, included ActivTrak, BrowseReporter/Currentware, WorkTime, Teramind, Time Doctor, Traqq Connecteam and many more. Such software enables employers to track daily work activity and long-term trends in productivity, to generate productivity metrics on a group or individual scale. In addition to the standard functions, these software also offer greater insight to evaluate productivity levels amongst employees. Employee monitoring software can vary in functionality. Features may range from having remote access/control of the remote or hybrid employee’s computer, to screen activity recording, employee activity monitoring, productivity analysis, browsing history, employee email monitoring, and time tracking software (Capterra, 2023). Some software may offer all these features (or more), while others may only offer a select few. To contextualize the ways in which some of these features are used, for example, Connecteam enables the employer to “easily monitor what your team is working on, when and from where”, “monitor if your employees are where they are supposed to be” and “have all past routes saved on the cloud and accessible” (Connecteam website,2022). Software like BrowseReporter allows the employer to “automatically captures screenshots of employee desktops”, “see exactly what your employees are doing on their computers” and “...capture screenshots when specific websites or applications

are used" (Currentware website, 2023). Traqq similarly offers this feature, as it "randomly takes screenshots every 10 minutes and stores them in a secure online account" and allows managers or administrators to access a screen recording feature, that will "capture 10-second videos of screen activity at random intervals" (Traqq website, 2023). Software like Traqq have the ability to "detect and report the apps and websites a user spends more than 10 seconds on" and display the information in the form of a pie chart, summarizing the most frequented websites and apps, enabling employers to "get insights into what's wasting time and take measures to restore efficiency", in addition to monitoring and reporting activity levels "by tracking mouse movements and keyboard clicks" (Traqq website, 2023). Other software enable email monitoring and capturing incoming or outgoing emails (see Figure 1 for TeraMind Email Monitoring example). Software, such as Time Doctor, monitors work progress even when offline or disconnected, and will "sync information to your account" when the user is back online, with tracked time and screenshots displayed on one's report (Time Doctor website, n.d.). Moreover, in addition to discrepancies in software used, Canadians employed in the private sector may be granted work-issued equipment to carry out remote work, such as computers, work phones, or tablets, however, others may be required to use personal computers and cellular phones to work from home (Obada-Obieh, 2022).

1.3 Concluding Remarks

In light of the significant shift towards remote work, the increased reliance on surveillance and monitoring technologies, the Canadian labour market has undergone profound transformation.

The standardization of telework brings forth a need to explore the implications of its regulation within the framework of a neoliberal governance paradigm and investigate the interplay between forms of power, job precarity, and individual privacy and security in the Canadian context. Drawing on a Foucauldian conceptual framework, the examination of the Canadian case, vis-à-vis the case of Greece, aims to address the following research question: How does the formulation of policy under a neoliberal governance paradigm influence the legal frame and policy instruments employed to achieve the policy goal? And, with respect to regulating teleworking technologies and procedures, how may the application of such a neoliberal approach potentially pose limits on the practical implementation of these policies?

Chapter Two: Theoretical Approach

By providing a comprehensive overview of the current state of knowledge, a Foucauldian approach to power allows for the contextualization of the current working conditions with the broader neoliberal framework. By examining the interconnection between precarious employment, the increase in demand for sophisticated surveillance technologies, and the prioritization of the state's economic well-being, the Foucauldian interpretive approach enables an in-depth examination of how disciplinary and security power reinforce one another, and the ways in which this dynamic supports and reinforced market-oriented principles.

2.1 Foucauldian Interpretive Approach

Foucault's contributions offer well founded analytic devices and interpretations (Keely, 1990) to assess social and organizational order, and thus the implications of the employment of power in the context of public administration. Foucault's contributions to the study of public administration frame the employment of two different types of power, disciplinary and security, with regard to telework and the development of *Bill C-27.* Also to mention is Foucault's contributions to the concept of governmentality. Neoliberal governmentality, from a Foucauldian approach, can be described as a fundamental rationale that provides guidance and informs the decision-making processes within the governing regime (Hofmeyr, 2022). This development, or "governmentality", denotes a different configuration of sovereignty, discipline, and government, bringing forth a new way to execute the practice of governance (Cawley and Chaloupka, 1997). Foucault's depiction of governmentality instills the political economy, an economic rationality, as the primary form of knowledge (Elden, 2007). As opposed to operating hierarchical authoritative approach to regulation, neoliberal governmentality attempts to generate a self-

regulating system by applying a decentralized, bottom-up, governance technique (Hofmeyr, 2022), thereby returning to the concept of panopticonism and surveillance as apparatuses utilized to ensure discipline and compliance, enabling the state to exert biopower over the population. Biopower, a management technique, is an essential element to this governmentality, as it facilitates the establishment of stability, enabling individuals to behave within appropriate boundaries without direct coercion. Biopower enables regulation over individuals' bodies, social behaviors, habits, and overall practices. The administration of individual human bodies, collectively, ultimately facilitates optimization of productivity at the broader, societal level (Foucault et al., 2008). Overall, Foucault's concept of governmentality encompasses a unique approach to governance, that of which shifts away from placing an emphasis on legal prohibitions and instead relied upon a comprehensive administrative structure. This structure enables management over both the population and the economy through a combination of disciplinary methods and security measures, with frequent prioritization of disciplinary methods (Foucault and Burchell, 2009). By adopting a Foucauldian framework for this study, the current neoliberal paradigm, in which policies are formulated, offers a foundation for the conceptualization of the issue at hand. A paradigm works as an interpretive framework that embraces certain principles, ideologies, and standards. This underpinning greatly influences how social issues are perceived, how policy goals are identified, and the types of instruments required to attain said objective (Hall, 1993). As such, it is valuable to pay attention to the greater political ideology, along with its underlying goals and elemental instruments, that framed the approach to digitalization in two different regards: the approach taken by private-sector organizations to expand and establish the digital workplace environment, as well as the management practices involved, and, secondly, the federal approach to policy making with respect to the Digital

Charter. The former will be approached with the concepts of disciplinary power, of which takes place at the micro-level, while the latter with that of security power, taking place on a macro-level. Together, the interplay of the two forms of power can serve to assess the administration of the current developments occurring in the digital arena.

2.1.1 Disciplinary Power

With the ideologies of neoliberal economics replacing Keynesian economics and the welfare state, the precarity-inducing, competitive economic policies are mirrored internally, within organizations. The precarious conditions of employment give rise to worker self-optimization, through disciplinary power and, in turn, through a managerial technique of surveillance (Farmer, 1995). Neoliberalism held, and continues to hold, a "disciplinary logic of capital" (Robins and Webster, 1999, p. 56). Individuals also come to exercise power over themselves without overt or direct coercion. In this regard, the panopticon can be viewed as a standard model for governance over the labour force (Gane, 2012). With set limitations to government interference and reduction in unionization rates (Pupo et al., 2012), job insecurity often results in greater levels of discipline and productivity. Noting that discipline, Foucault argues, is "central for achieving positive economies, through a detailed internal arrangement, maximum efficiency and speed in the use of time" (Foucault, 1977, pp.149-155 as cited in Sargiacomo, 2009). The pandemic has exacerbated economic and financial precarity, and, in addition, the implementation of panoptic surveillance has been remarkably facilitated by the mass shift to telework. Panoptic settings typically comprise a focal point of watch and power. Foucault expanded significantly on Jeremy Bentham's panopticon, architectural design of institutions, and architecture as a means of organization and control. Given the organization and control that institutions produce in relation

to their structure, it renders them political in nature (Foucault, 1980). Throughout this study, the principle of architecture and panoptic surveillance is applied. This principle is applied not despite the lack of physical architecture granted to the arena of telework, but rather because of this. With the progressive diminishment of the physical workplace and the increasing development of telework-facilitating technology, the evolving technology has the capacity to reinstate an organization's architectural design in a way that faces no physical boundaries in space or time. Foucault focused on how the configuration of a particular environment can serve as a mechanism to exercise power. As such, the use of panoptic surveillance renders physically coercive measures unnecessary and drives individuals towards self-regulating behaviour:

> "There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by interiorizing to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost" (Foucault, 1980, p. 155).

Disciplinary power, overall, is founded on three main elements: hierarchical observation, the normalization of judgment, and examination (Sargiacomo, 2009). Examination, however, is a process, combining the techniques used in observation and judgment (Sargiacomo, 2009). The mechanism of examination be synthesized through three main features:

> "(a) being the examination process highly ritual, a compulsory visibility is assigned to the examined subjects; (b) a mass of written documentation and records is central for the examination of the individuals, who are thereby embedded into the field of documentation; (c) being inserted in a network of writing, and described by piles of documents and records, any individual becomes a single case, which can be judged, measured and compared with others" (Sargiacomo, 2009, p. 275)

Thus, examination is the process enabling the mobilization of hierarchical observation and the normalization of judgment, in turn, enabling those who possess disciplinary power the ability to assess, categorize, and penalize individuals. This exercise of power, Foucault argues, is profoundly embedded in economic relations (Foucault, 1980). Academics Robins and Webster called attention to panoptic surveillance, arguing that "the panopticon is the precursor for

Scientific Management" (Robins and Webster, 1993, p. 245), as Taylorism employed surveillance as a form of control and as a means to achieve productivity to the most feasible extent (Robins and Webster, 1993). Competition, rooted in efficiency, serves as a major driving force in self-regulation, creating order on a micro level, within organizations, and on a macro level, in the larger economic market, noting that discipline, Foucault argues, is also "central for achieving positive economies, through a detailed internal arrangement, maximum efficiency and speed in the use of time" (Foucault, 1977, pp.149-155 as cited in Sargiacomo, 2009). The use of flexible and market-oriented mechanisms can be considered a form of the biopolitical control of neoliberal governmentality, contingent on "tuning and shifting the market competition, using flexible and market-based forms of control, while concealing and de-politicizing through technical coding, which modifies competition within the market, rather than regulating top-down" (Törnberg and Uitermark, 2020, p.6). It is thus valuable to consider the vastitude of achievable panopticonism in the contemporary private-sector labour force through the various technologies employable through teleworking software (Katsabian, 2020). As private-sector management fears a decline in productivity levels while working from home (Barbara et al., 2020), many organizations turned towards control over productivity through actual or perceived continuous surveillance and monitoring due to the remote nature of telework. The development of new technologies become increasingly intrusive and progressively capable of penetrating the public sphere into personal areas (Katsabian, 2020; Robins and Webster, 1993). A Foucauldian analysis of employee surveillance enables the foundation to conceptualize the power granted to management in increasingly panoptic workplace environments.

2.1.2 Security Power

Foucault's theory on security power, though understudied in comparison to disciplinary power, will additionally serve to frame the technique trailing policy making relative to the Digital Charter. Under disciplinary power, the objective is to secure obedience by regulating and controlling individuals at an individual level, whereas security power executes itself on generalized terms, as it "works at the level of the imaginary reality" (Foucault, 2009, p. 47, as cited in Togman, 2021, p. 223). The use of security power can be understood as "a matter of maximizing the positive elements and minimizing the risky or inconvenient while knowing that they will never be completely suppressed" (Foucault, 2009, p.19, as cited in Togman, 2021, p. 233). Thus, security power strays away from the sovereignty over individual behaviour and leans into the government of populations, creating "two completely different systems of power" (Foucault, 1977-78, p. 66, as cited in McNicoll, 2007, p.830). Foucault characterizes security power as a method to answer how to maintain socially and economically acceptable behaviour at a level sufficient enough for society to function adequately (Togman, 2021). Thus, as opposed to disciplinary power, security power operates in a decentralized manner, regulating as little as possible, thereby embracing a laissez-faire approach to policy implementation (Elden, 2007). Under the influence of security power, the state disengages from micro-level affairs and focuses on the broader aspects of society (Togman, 2021). The governance macro-level affairs appear to govern an "abstract entity" (Togman, 2021, p. 238), ultimately detached from realities occurring on a micro-scale. Policies created oftentimes fail in their effectiveness and fail at achieving its objectives due to the profound gap between macro-level policy and individual realities (Togman, 2021). Here, apparatuses of security take the form of an essential instrument to the political economy remains a major form of knowledge, with the population, as a concept as opposed to a

collection of subjects or individuals, set as the target (McNicoll, 2007). This approach illuminates the interplay between security measures and the broader socio-economic landscape and its pertinence to the study of public administration, granting an in-depth examination of governance approaches.

2.3 Concluding Remarks

Foucault's theories of power, both security and disciplinary power, separately and interactively, will therefore serve as analytical frameworks and will be employed in this study to comprehensively examine and assess the developments made with *Bill C-27.* The concepts of security and disciplinary power under neoliberal governance will be instrumental in addressing the research question as they help frame the rationale supporting the development of the Canadian Charter. By understanding how these concepts have been pivotal in influencing the Canadian approach to regulation, it also facilitates the examination of Greece, and how its approach appears to have deviated from this approach in its own legal framework for teleworking.

Chapter Three: Research Methods

In order to assess the ways in which a neoliberal governance paradigm shapes policy formulation and its subsequent practical implementation, this study looks at two separate cases, that of Canada's Digital Charter and that of Greece's framework put forth by the HDPA.

3.1 Multi-Case Study

This study uses secondary research as the research method. This method was chosen in order to make use of existing information to conduct a case study of Canada's Digital Charter, in comparison to Greece's teleworking policies. In order to do so, this study makes use of a multi-case study research. Case studies allow research offers a method for evaluating decisions undertaken. This is carried out by analyzing their purpose, how they were taken, and their implementation (Schramm, 1971, as cited in Yin, 2017). As such, through the examination of the Canada's Digital Charter and HDPA's legal teleworking framework, insights into the influence of governmentality in decision-making, the structuring of policy instruments seeking to meet the policy objectives, and thus its implementability. As such, this two-case study, both presented in separate sections, will be analyzed together by way of a cross-case analysis. The interpretation of these results enables drawing conclusions based on the analysis, guided by the Foucauldian approach, in order to further mobilize these findings with respect to identifying potential gaps in Canada's Digital Charter. By carrying out a multiple case study and a cross-case analysis of Canada's *Bill C-27* alongside Greece's teleworking framework, of which will serve to establish a point of reference and benchmark, will enable grounds to assess the implementability of the

digital charter. Thus, in sum, through the examination of Greece's approach to policy implementation, this secondary research offers the opportunity to identify gaps and assess how Canada may benefit from Greece's initiative by way of policy transfers, be it emulation of policies, direct copying of policies, or general inspiration (Dolowitz and Marsh, 2000). The purpose of selecting Greece is to showcase its pioneering approach to regulating privacy and security by way of reforms in labour laws in relation to telework. Moreover, Greece's approaches are significant to note, particularly due to its unique deviation from the neoliberal paradigm, in consideration of its position as a developed economy. Greece has experienced significant disputes and disagreements in the process of undergoing neoliberal reforms (Kennedy, 2016). While Greece has yielded to the pressures from the broader European agenda to implement labor market reforms aimed to deregulate the labour market to increase competition, it has consistently displayed resistance to internalizing a neoliberal macroeconomic policy paradigm throughout its history (Gönenç and Durmaz, 2020; Kennedy, 2016). In this regard, it is valuable to consider the policy implementation within a country that operates within the same macroeconomic context but demonstrates resistance towards fully embracing its underlying doctrine.

3.2 Technique

In order to carry out secondary research and, this study therefore undertakes a multi-case study with a cross-sectional analysis. The case study attempts to examine the recent developments of *Bill C-27,* and rationale underlying the set of decisions taken, in addition to the illuminating the

rationale and decisions taken by the HDPA. The cross-sectional analysis will facilitate the evaluation of implementability of the proposed regulations, with respect to the policy instruments used to carry out the policy objective of privacy and security of non-federally employed individuals.

The particular sources consulted include documentary information, including administrative and legal documents, such as *Bill C-27,* PIPEDA, the HDPA's legal framework, and the Government of Canada's National Digital and Data consultations, and reports issued with respect to privacy from the House of Commons Canada. Moreover, it also includes archival records, such as secondary data and publicly available data records from the Office of Privacy Commissioner (OPC) of Canada and Statics Canada. In order to retrieve the archival record sources and to retrieve relevant literature for review, the major data collecting instrument used is the Omni search tool for the University of Ottawa library was used. The tool searches the institution's library, along with 17 other databases that it is subscribed to. To ensure that the relevant articles were procured, synonyms of "telework" were utilized as search terms, such as "remote work", "telecommuting", "work from home", "virtual work", and "telecommute jobs". Moreover, search terms such as "surveillance", "monitoring", "panopticonism", "power relations", "equity", "worker rights", "security", "privacy", and others were used in order to identify the main concepts pertaining to the topic of research. As this issue is fairly recent, it was important to recognize that articles were published prior to the emergence of Covid-19. It was also important to identify the position the authors held in describing digital work issues, due to the environment of digital work, and thus its slower-pace evolution, at the time of writing. The data selected for this study was published post-Covid to have an accurate depiction of

contemporary digital work conditions. All information published before the pandemic was selected intentionally to highlight the degree of change in perception, understanding, and extent of remote work.

With respect to retrieving the legal documents at the core of the cases under study, legal and official Canadian documents and government-produced information, information was retrieved from the House of Commons Canada webpage (OurCommons.ca) and federal webpages, including the official website of the OPC (Priv.gc.ca) and the official websites of Innovation, Science, and Economic Development Canada (ISED) (ISED-ISDE.Canada.ca). Both websites grant the user the option to search publicly available records by matching the criteria entered in the search box. The OPC website offered a direct link to the webpages of provincially regulated privacy policies in select provinces. The legal and official Greek documents and government-produced information were available on the Hellenic Data Protection Authority webpage. The guidelines on the "application of personal data protection rules in the context of teleworking" (Greek: Σχετικά με την εφαρμογή των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της τηλεργασίας), an official document by the Hellenic Data Protection Authority, was solely accessible in its original language. As such, many of the documents required to conduct the case study were exclusively available in the Greek language. Machine translation software was used to translate the documents. In order to ensure the accuracy of translation and interpretation, three different translation tools were used: Google Translate, DeepL Translate, and SYSTRAN Translate.

3.3 Benefits and Limitations

3.3.1 Benefits

The benefits of secondary research within this study lie within its ability to gather available information, or importantly, the lack thereof, and analyze to uncover the cause and consequences of inadequate or insufficient teleworking policies. Therefore, this secondary research gathers and organizes information in a manner that provides the capacity to examine movements, initiatives, and overall trends in government regarding the digital transformation. As teleworking in the post-Covid era is fairly new, secondary research provides an opportunity to pull from various data sources, enabling the assessment of the current state of Canadian policy in order to formulate a basis for proactive policy change and/or reform. In the scope of public administration, this method of research provides practicality and a basis for further research. The use of both documentary information and archival records as sources for this case study offer stability, as the information can be reviewed multiple times, and unobtrusiveness, as they are not created as a direct result of the current studying, allowing for a more objective analysis (Yin, 2017). Moreover, the sources of information are simultaneously specific and broad, specific in the fact that it allows the identification of individuals involved, such as the professionals leading the 2018 consultation, the individuals comprising the Standing Committee on Access to Information and Privacy and Ethics in the deliberation and report carried out by the House of Commons. It is too broad in the way that this information covers a long span of time and events, seeing as that the consultation and development of *Bill C-27* were carried out prior to the

emergence of Covid-19, during, and post-Covid 19 restrictions. The archival records, specifically, offer quantitative data, offering objectivity.

3.3.2 Limitations

Secondary research involves using data collected for a different purpose by other researchers or organizations. Consequently, the research questions or objectives may not align perfectly with the original intent of the data collection, leading to limitations in addressing specific research inquiries or exploring new perspectives (Thiel, 2014). As secondary research involves the use of data that has been collected for different purposes, the alignment of the research question and the original intent of the data collection may result in a lack of precision. Moreover, a limitation encountered in this research paper, specifically regarding archival data was the inability to access individual responses submitted by survey respondents. Secondly, limitations with regard to available data on the Canadian population, excluding datasets provided by Federal agencies, were scarce in comparison to data available deriving from a studied population in the United States. With respect to documentary information, a language barrier regarding the HDPA's framework was encountered, as this document, in particular, was solely available in the Greek language. Overall, a significant limitation to note is the scarcity of Canadian academic research in this field. The intent behind data collection with Federal agencies differ from the purpose of this paper, along with the limited Canadian data produced otherwise, rendering this limitation rather insightful in the assessment of the implementability of *Bill C-27.*

3.4 Concluding Remarks

By employing a multi-case study and conducting cross case analysis, guided by a Foucauldian lens, this methodology serves to establish a solid foundation to evaluate the different approaches taken to regulating the on-going advancements made in the digital sphere. By reviewing relevant literature and providing a background on labour laws through PIPEDA, in addition to data records from the OPC, ISED's consultations prior to the development of the Bill, and reports issued with respect to privacy from the House of Commons Canada, this method provides the grounds to identify potential gaps into Canada's Digital Charter. Foucault's notions of governmentality, disciplinary, and security power, provide the conceptual framework for shaping methodology and analysis employed in this study. Delving into two separate cases of regulatory measures undertaken provides significant insight on Canada and Greece's respective approach to governance over personal data, privacy, and security in light of escalating digitalization.

Chapter Four: Description of Cases

Both the Digital Charter and the HDPA have aimed to reform and enforce a regulatory framework set out to address concerns over personal data, privacy, and security, amid the rapidly evolving digital landscape, characterized by technological integration and data-driven practices. Although the regulatory frameworks may appear to considerably similar at first glance, a closer examination reveals distinct and substantial differences in their respective approaches. This chapter aims to introduce the Canadian developments and the Greek developments in their initiative to ameliorate individuals' rights in the digital age.

4.1 Canadian Privacy Laws and Policies

4.1.1 Administration of PIPEDA

In Canada, ground rules for the ways in which private-sector organizations collect, make use and disclose personal information, defined as "information about an identifiable individual" (Personal Information Protection and Electronic Documents Act, 2000, p. 4; Digital Charter Implementation Act, 2022, p. 5) are set out in the federally administered Personal Information Protection and Electronic Documents Act. Examples of what personal information entails, as provided by the OPC (2019), include age, names, identification numbers, income, blood type, ethnicity, credit and loan records, medical records, and political opinions. The administration of regulatory enforcement of privacy rights is determined by several factors. As indicated by the OPC (2018), the enforcement of privacy rights and laws is determined by 1) nature of the organization processing personal data, be it a federal government institution, a provincial or

territorial government institution, private sector, or a federally regulated business; 2) the geographical location of where the organization is based; 3) the type of information involved; and 4) whether or not the information involved crosses provincial or national borders. PIPEDA is governed by the OPC and therefore oversees the compliance and enforcement of privacy rights. PIPEDA does not apply to all provinces and territories as a matter of course. Not all issues of privacy are under the oversight of the OPC. The provinces of Alberta, British Columbia, and Québec operate under their own private-sector policy laws (which, according to the OPC, have been deemed substantially similar to PIPEDA) and are overseen by their respective Office of Information and Privacy Commissioner.

4.1.2 The 2018 National Digital and Data Consultations

On June 19, 2018, the Government of Canada launched its National Digital and Data consultations of which played a significant role in the development of the Digital Charter Implementation Act in 2022. The consultation was put forth to improve democratic governance, enabling a platform for Canadians to consult on the public policy issue: the future of work in an increasingly digitalized environment. The 2018 consultation was a result of the Canadian Government's plan to develop a plan for economic growth, and for Canadians to be employed and succeed in the competitive economy. More specifically, purpose of the consultation was to examine ways for Canada to promote digital innovation, equip Canadians for a digitalized future of work, and instill trust and confidence in how data is being used (Government of Canada, 2019). The overarching goal for the Digital and Data consultation was geared towards making Canada a competitive, data-driven, digital economy, founded on six business-led Economic

Strategy Tables. Participants were organized into four groups: Women, Indigenous Peoples, New Canadians, and Seniors. The Digital Engagement Leaders comprised of six individuals: Janie Béïque, Executive Vice-President, Investments at Fonds de solidarité – Fédération des travailleurs et travailleuses du Québec (FTQ; Quebec Federation of Labour), the largest development capital network in Quebec; Dr. Arvind Gupta, professor of Computer Science at the University of Toronto, with extensive publications on computational genomics and national innovation and industrial strategies; Dr. Sarah Lubik, Director of Entrepreneurship for Simon Fraser University, with expertise in entrepreneurial education and commercialization; Carole Piovesan, lawyer at the McCarthy Tétrault Canadian law firm and lead in the area of artificial intelligence; Mark Podlasly, founder of Brookmere Management Group, helping Indigenous and local communities identify and engage economic, social and educational opportunities; and Dr. Ilse Treurnicht, with expertise in commercialization, growing technology firms, venture capital and social finance, in addition to public policy development (Government of Canada, 2019). Topics discussed in regard to future actions to undertake in developing an inclusive digital and data-driven economy included 1) Digital and Data Transformation; 2) Digital and Data Transformation (for youth); 3) Unleashing Innovation; 4) Trust and Privacy; 5) Future of Work; 6) Future of Work (for seniors); 7) Immigration; 8) Being Human in the Digital Age; 9) Supporting and Empowering Women; 10) Provincial and Territorial Perspectives; 11) Canadian Opportunities for Leadership in the Digital Economy; 12) Indigenous People; and 13) The Future of the Digital Economy (Government of Canada, 2019). Responses from women, in summary, pertained to policies supporting and promoting work-life balance. Responses from Indigenous Peoples, pertained to access to affordable and reliable digital infrastructure, the

elevation of the digital divide, and the necessity for Canada to include Indigenous Peoples in Digital and data transformation as per the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). New Canadians expressed concern over difficulties keeping pace with demand for skilled labour, and the importance of having the digital skills necessary to remain competitive in the digital economy. Senior Canadian citizens expressed concern over social isolation and complicated processes involved in the expansion of digital and data-driven technologies (Government of Canada, 2019). Generally, Canadians emphasized the importance of adequately equipping the younger generation for the evolving workplace landscape, as well as ensuring ongoing support for employees in acquiring new skills to facilitate career transitions throughout their lifetimes. Concerns were also voiced regarding affordability and access to high-speed Internet. However, even prior to the national mass transition into teleworking, Canadians still expressed worry over how personal data is being utilized and collected. The Government acknowledged this concern by stating that PIPEDA required reform and modernization. Concerns expressed by Canadian citizens and responses made by the Canadian Government pertaining to a changing labour model were articulated in the context of skill and talent with new technologies. Thus, labour-related dialogue remained in the scope of skill gaps and digital skills/literacy. Trust, privacy, and personal data were discussed in the context of Canadians requiring the necessary information tools and digital literacy to make well-informed decisions online. It was also discussed in the scope of developing international privacy norms and regulations for technologies, such as open banking or blockchain, due to the disruptive innovation it brings to the Canadian market. These international policies were suggested to be carried out through international collaboration and alignment of the General Data Protection

Regulation's (GDPR) existing framework, of which establishes general obligations regarding the processing of personal data, implementation of appropriate security measures proportionate to the risk involved in data processing operations (European Parliament, 2023). Overall, as the consultation took place prior to the emergence of COVID-19, the labour market model of "a standard- 40 hour workweek, working with a building or factory" (Government of Canada, 2022) had not yet undergone a substantial transformation, the overarching concepts of labour and privacy had not been associated.

4.1.3 Recent Developments in Canada's Implementations of the Digital Charter: Bill C-27

In 2022, ISED put forth the Digital Charter to strengthen Canada's private sector privacy law. The Canadian Federal Government thus passed *Bill C-27*, The Digital Charter Implementation Act: An act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act, and, in order to make consequential and related amendments, enabling a foundation for the development of the Digital Charters for protection of personal information framework reform. The 2022 Digital Charter Implementation Act introduces the proposition of the three following Acts: The Consumer Privacy Protection Act (Part 1 of the *Bill C-27*), the Personal Information and Data Protection Tribunal Act (Part 2), and the Artificial Intelligence and Data Act (Part 3).

The Consumer Privacy Protection Act would replace PIPEDA in delineating the obligations of commercial organizations regarding the management of personal data (OPC of Canada, 2023) and aims to protect Canadians while ensuring that businesses have clear rules to follow as technology evolves. To do so, it intends on regulating facets of digital technology,

including enhancing the level of regulation and transparency of organizations in the handling of personal information; making certain that Canadians have the ability to demand the disposal of their information once it becomes unnecessary; introducing stronger safeguards for minors, such as restricting the collection or utilization of information about minors and holding organizations at a higher standard for the handling of minors' information; providing the Privacy Commission of Canada with the authority to order a company to cease collection data and using personal information; and establishing non-compliance fines of either 5% of global revenue or $25 million, whichever is greater (Government of Canada, 2022). More specifically, Part 1 of the Bill focuses on the flow of personal data through geographic boundaries, thus, applying to personal information that is collected or disclosed internationally or interprovincially by the organization in the course of commercial activities (*Bill C-27*, 2022). It articulates that organizations are accountable for the personal information that is under their control and that organizations are required to establish and uphold a privacy management program encompassing the policies, practices, and procedures to maintain their obligations under the Act, including:

> "(a) the protection of personal information;
> (b) how requests for information and complaints are received and dealt with;
> (c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and
> (d) the development of materials to explain the organization's policies and procedures." (*Bill C-27* 2022, p. 9)

Moreover, the Act aims to protect personal information about an employee or an applicant for employment and highlights that organizations may use or disclose information in an appropriate manner and for reasonable purposes. The purposes should represent a legitimate necessity for the organization, and it must consider whether there are alternative methods with lesser intrusion that may accomplish the objective at a similar cost and comparable advantages. It must also consider

whether the individual's privacy loss is proportional to the benefits considering the measures implemented by the organization to alleviate the impacts of the individual's loss of privacy. The Act does not apply to organizations with respect to data collection of an individual's personal information, that the organization collects and uses for the purpose of communication or facilitating communication in relation to their employment. With respect to limiting collection and use, organizations are required to determine at the time or before the time of collection, the purposes for collecting said personal information. However, should organizations use AI for the purpose of decision making ("automated decision system"), defined as any technology assisting or replacing the judgment of human decision-makers, the organization must make the information available, on a general account, with regard to its use. Organizations are also not authorized, without the individual's consent, to access a computer system to collect or use personal information through any means of telecommunication or to cause a computer system to be accessed.

The objective of the Personal Information and Data Protection Tribunal Act is to facilitate the enforcement of the Consumer Privacy Protection Act by enabling recommendations made by the Privacy Commissioner of Canada to be reviewed by the tribunal. This would allow for the enforcement of monetary penalties for certain violations. Lastly, the Artificial Intelligence and Data Act, a newly introduced concept to the Canadian Federal Government's administration of the use and collection of personal data, intends to strengthen Canadians' trust in both the deployment and development of AI-based systems by regulating international and interprovincial trade and commerce. This act aims to apply rules to the use of AI, including ensuring that AI systems with significant impact are created and implemented in a manner that recognizes,

evaluates, and minimizes potential risks of harm and bias; establishing an AI and Data Commissioner to assist ISED's Minister in executing ministerial obligations, including monitoring companies' compliance, mandating or ordering third-party audits, and disclosing information to other regulatory bodies and enforcement agencies as needed; and outlining comprehensive criminal prohibitions with respect to the use of unlawfully acquired data for the development of AI-based systems or in situations where imprudent AI deployment would pose serious harm, where substantial economic loss may be of result (*Bill C-27*, 2022). Overall, this Act also intends to regulate international and interprovincial trade commerce in AI systems, by establishing common requirements pertaining to its development. Content that is generated through AI systems must not produce biased output, cause physical or psychological harm, damage property, cause economic loss to an individual, or operate at odds with the *Canadian Human Rights Act* (*Bill C-27*, 2022). Should the AI system meet the criteria for a high-impact system, the person responsible for it must identify, evaluate, and mitigate the risks of harm or biased output. At the same time, the person who is indeed responsible for the AI system must assess whether it is a high-impact system. The criteria of what constitutes a high-impact system has yet to be defined.

4.2 Labour Law and Privacy Regulation Reforms in Greece

The public administration of Greece has not been a commonly studied subject in social science-related disciplines and has only recently caught some attention (see Spanou, 2020). Furthermore, teleworking was not a common phenomenon in Greece until the Covid-19 pandemic. Since the pandemic, the frequency of online activities has increased largely due to

teleworking, alongside video conferencing (Mouratidis and Papagiannakis, 2021). Prior to the involuntary adoption of telework, 40.3% of the studied population in Greece had never teleworked, whereas 47% have reported to have teleworked every day since the pandemic (Mouratidis and Papagiannakis, 2021). On June 19, 2022, Greece introduced major reforms to its employment legislation (Industrial Relations and Labour Law, 2021). This is the first-time labour laws have been updated since 1982 (Industrial Relations and Labour Law, 2021) at a time when the mere idea of teleworking through the Internet was a new concept (Industrial Relations and Labour Law, 2021). The legislative framework reforms on teleworking addressed teleworking in not just the public sector, but also the private (Bakirtzi, 2022). Greece admitted that the framework pre-pandemic was outdated and did not adequately respond to the new reality of work (Bakirtzi, 2022). As such, Greece has carried out major reforms, introducing law 4808/2021 to modernize employment law alongside social and technological changes and challenges in the Greek market. The HDPA is a constitutionally established public, regulatory authority, which acts to ensure that the application of the GDPR and other regulations regarding protection of the individual from the processing of personal data is carried out. The legal framework for remote employment thus works alongside the legislation on the protection of personal data by incorporating the European-level legislation (the GDPR) in the scope of electronic communications.

4.2.1 Legal Framework for Teleworking in Greece

The Hellenic Data Protection Authority guidelines pertain to provisions and regulation of personal data protection in the context of teleworking (2021). It was issued to take greater

security measures and acknowledge the risks inherent to Information and Communications Technologies (ICT) and the intensity and extent that remote work has taken since the emergence of the Covid- 19 pandemic (HDPA, 2021). The guidelines aim to shape the provisions of data intake and processing for remote work and address remote working conditions for both public and private sector employment (HDPA, 2021). The guidelines consider a wide range of factors. The main themes attributed are 1) transparency, 2) necessity, 3) equity, and 4) surveillance.

The provisions of data intake set out by the HDPA allocate high levels of accountability over to the "controller", i.e., the one holding control over data collection. As such, the controller is expected to inform the employee of personal data being collected, and that this data is limited to only what is necessary for operational purposes. Moreover, the employee must be transparently informed of the risks of teleworking. The guidelines explicitly articulate that the organization of remote employment must not lead to inequalities or discrimination, such as salary, career development opportunities, and participation in professional development programs training, nor should it have implications on employment insurance and the social rights of employees. On a similar note, the guidelines also indicate that remote employment should not lead to further automated decision-making regarding individuals, including the profiling of remote employees. The HDPA particularly highlights the greater potential for inequality, discrimination, and threats to the social rights of employees employed within the private sector due to existing power imbalances inherent to private sector working conditions. Regarding the organizational and technical measures, the legal framework for teleworking in Greece states that the controller is required to continually attune the organization of remote work according to the new [working] conditions emerging from the advances in telework and must demonstrate

compliance with the GDPR's greater Framework of Accountability. In this context, technical and organizational measures must be established prior to acquiring and processing personal data. Thus, delays in responding to the exercise of rights by the employees, require the controller to formally document reasons for delay or non-satisfaction of the exercised rights. Continuous surveillance of the employee, through the obligation to operate the use of the computer camera (webcam) and the use of AI software, such as facial and/or motion recognition, 'screen sharing' or the use of keystroke logging software, or any obligation for the employee to perform regular actions to prove their presence behind the screen. In a series of its decisions, the HDPA has deemed forms of continuous surveillance of this nature could hardly be qualified as complying with the principle of proportionality. And in regards to the use of a webcam for performance monitoring, the controller is only permitted to do so in an instance in which it is necessary for the protection of persons and/or property. Therefore, data collected through computer cameras may not be used as a criterion for the performance assessment of the employee. Recordings of teleconferences must be carried out solely on the basis of the employee's work and telework contract obligations, and therefore also on the principle of proportionality. In regard to videoconferencing, both private and public sector employees are entitled, in the application of the principle of data minimization, to participate in virtual meetings only through a microphone. Continuous participation in visual meetings via camera is not mandatory and, should webcams be used, it is recommended that employees choose to blur their backgrounds or use alternative images, to avoid revealing personal information. Overall, the guidelines implemented by the HDPA are, to a great degree, comprehensive and meticulous, encompassing a wide range of aspects related to modern-day teleworking. Its precision on privacy regulations can serve as a

valuable resource in Canadian policy development in promoting a secure and equitable digital work environment.

4.3 Concluding Remarks

The Canadian Digital Charter and the HDPA have both attempted to address the issue of privacy and security in private sector organizations. The regulatory documents cover similar grounds, with similar objectives, such as safeguarding individuals' personal information to uphold their privacy rights in an increasingly digitalized space. However, despite their similar objectives, the frameworks diverge considerably in their approach to achieving said goals. The HDPA has taken an authoritative, top-down approach to asserting direction to which private sector employers are required to adhere to. It has established specification through the articulation of boundaries, limitations, and accountability. In doing so, the HDPA's framework provides a clear code of conduct governing the organization's operational practices. The framework carves out specific boundaries within which employers are required to adhere to. The Digital Charter, despite its intent to impose regulations on the private sector organizational operations and employer behaviour, particularly with the use of AI systems, makes no mention of remote work, or synonymous terminology. Acknowledging that it is indeed broader in scope, the ambiguity presented in the Digital Charter, in contrast to the restrictive boundaries put forth by the HDPA, nonetheless prudently refrains from imposing overly stringent restrictions to avoid potential consequential retrains on economic activity, thereby minimizing significant interference and preserving organizational resources. In doing so, however, this may have considerable implications on its practical implementation. Thus, despite the similarities in objective, the governance paradigm under which the Digital Charter has been developed holds great influence

over its administration. As this study delves further into the analysis, it will seek to uncover the ways in which a deep-seated neoliberal policy paradigm has significantly influenced the development of policy and policy instruments.

Chapter Five: Analysis

The preceding chapters attempted to demonstrate the implications of neoliberalism and the facilitation of surveillance-based behaviors on an organizational scale and a macro, governmental scale. While these issues can be distinguished from each other, there is significant value in examining them as a unified subject of discussion, and thus through examining the political economy, the past and present role of teleworking, current state of technology, and the overarching privacy, security, and equity concerns. By adopting a Foucauldian approach to the theoretical framing of the study, the subject matter can be dissected through key Foucauldian concepts. The preceding chapters have thus sought to highlight the interplay between neoliberal governmentality and panoptic surveillance in the digitalized era, along with their consequential implications, which can be characterized by discipline and biopower**.** This chapter aims to carry out a cross-case analysis, assessing the Digital Charter framework with that of the HDPA's through the use of the Foucauldian framework to identify the ways in which the Foucauldian concepts of power, of which are embedded in political and economic rationality, are mobilized throughout. As disciplinary and security power are pivotal techniques utilized within the neoliberal governance paradigm to maintain and uphold market-oriented principles, these concepts, or the lack thereof, will serve to guide the analysis and assess the differences between Canada and Greece, particularly with the references made to AI and the collection of personal data.

5.1 Cross-Case Analysis

With *Bill C-27* and the greater push towards establishing a digital charter of rights, this policy area has been increasingly considered in contemporary policy development. However, there remains substantial opportunity for further improvement. Though some progressive reforms are proposed, such as the substitution of PIPEDA with the Consumer Privacy Protection and the introduction of third-party audits to monitor compliance, it nonetheless exhibits potential gaps that warrant attention and further consideration. The data presented has demonstrated the ways in which the private sector's approach to telework has fallen short of establishing clear standards. Neoliberal governance leaned into deregulation in order to achieve self-regulating markets, heavily driven by competition. By reducing social protection in the labour markets, mechanisms of precarity and competition aim to establish and maintain high levels of employment (Kennedy, 2016). As organizations increasingly seek to tools to establish disciplinary power and maintain productivity in remote work, as shown in the substantial surge in demand for surveillance-based technologies by employers (Masoodi et al., 2021), they have ventured into a large and unregulated market of surveillance technology, of which has been shown to be a 2.2-billion-dollar industry (Masoodi et al., 2021). Despite the shared surveillance and monitoring aspects, the abundant telework software programs exhibited substantial variations. Moreover, considering that approximately half of private sector enterprises operate on software unrelated to their industries (Statistics Canada, 2022), these organizations possess the autonomy to adopt telework in any manner they choose. This extends to the decision of whether employees are provided with company devices for remote work or required to use their personal computers and/or phones. The precarious characterization of many positions held in the private sector has facilitated the misuse of power within organizations. As employment stability is heavily determined by

individual performance, the use of surveillance and monitoring can be employed as an indirectly coercive mechanism to exploit compliance. Moreover, this mechanism can be optimized to its fullest extent through teleworking software and other instruments. The Foucauldian concept of disciplinary power, here, is instrumental to mobilize. Examination is central to safeguard against any diminishment in productivity and thus at the core of the rationale behind the demand for these software systems. Hierarchical surveillance has been amplified through the technological capacities employed in panoptic surveillance software programs. Secondly, the normalization of judgment has been identified on different accounts. Fear of embarrassment or other negative socio-organizational outcomes with respect to telework (be it due to non-compliance or error) have been identified (Obada-Obieh, 2022; Kwak et al., 2020). Hesitancy with respect to expressing discomfort over surveillance and monitoring practices and with respect to flagging suspicious calls or emails was largely correlated to the possibility of negatively impacting one's reputation caused by employer judgments. This discomfort remains marginally contested as a result of apprehensions surrounding employment stability (Obada-Obieh, 2022). The worries regarding judgements were founded on of potentially misleading productivity analytics (Catană et al., 2022).

5.1.1 The Use of Artificial Intelligence

Bill C-27, per the data presented, may potentially fall short or lack implementability as it may not serve to sufficiently focus on the foundational aspects. By mobilizing the concept of security power, the gaps between the contemporary nature and implications of telework and the Acts presented in the digital charter can be identified. Firstly, Greece’s historical resistance to wholly adopting a neoliberal paradigm has allowed it to displace the political economy from being at the

core of its governmentality, and therefore, from the center point in policy formulation, thereby departing from an exclusively economic type of rationality, This offers valuable insight on answering why Canada's Digital Charter may be too general in scope. With telework being one of the leading and involuntary sources of increased online activity, the government of Greece has confronted the negative privacy implications of working from home by releasing a framework precisely addressing this new form of work. The Artificial Intelligence and Data Act, and the Personal Information and Data Protection Tribunal as a part of *Bill C-27*, is a positive direction to take in regard to minimizing risks of deployment and development of AI systems. However, as the labour force has been vigorously marketed to and overall, substantially affected by digitalization, preventative instruments, and measures at the level of the employer and/or organization would offer greater safeguards for hybrid and remote employees. Additionally, it is important to note that the requirements state that a person who carries out the use of an AI system must establish measures with respect to the use of anonymized data, assess whether the AI system in question is indeed a high-impact AI system, and establish measures related to risks related to high-impact AI system. Moreover, it also requires the person who is responsible for the high-risk AI system to be establish measures to identify, assess and mitigate the risks of harm or biased output that may potentially result from the high-risk system, and is required to keep records describing their assessment. Each requirement is contingent on the individual data controller's assessment and evaluation, potentially leading to significantly varying results across organizations. While the Minister is entitled to conducting an audit, should the Minister have reasonable grounds to suspect that the requirements have not been adhered to, given the absence of standardized guidelines, this would likely require an internal whistleblower, i.e., an employee who would report misconduct. However, in the context disciplinary power, as the state of the

employment remains precarious and with increased monitoring and surveillance technology, this too may impede the ability or willingness to report a breach of adherence to the requirements. Previous research findings have emphasized the increase in reluctance to voice concerns around suspicion, due to worries of harming one's reputation at the place of work out of concern for their job security. In this context, this illuminates how the facilitation of disciplinary power within organizations may potentially impede the attainment of the initial objective. By accrediting organizations with the autonomy and responsibility to classify and delineate the affairs of AI systems within general parameters, there remains potential for considerably inconsistency, rendering it difficult to detect a breach of adherence to the predominantly self-imposed requirements. As the Bill does not explicitly establish guidelines to organizational surveillance and monitoring practices, thereby enabling further exploitation of disciplinary power, it may present a greater challenge for individuals seeking to confidentially report any suspected violations.

Without regulation over limitations with respect to the extent of surveillance and/or monitoring permitted, this may also weaken the enforcement of the Act's objective of reducing risks of harm and bias. This policy instrument, or the absence thereof in the case of digital charger, would serve as the mechanism enabling the connection between policy formulation and implementation (Ali, 2013), of which can be observed within Greece's framework. The HDPA's framework recognizes implications of the private sector, explicitly articulates what it considers to be inequitable or discriminatory practices, and preventatively restricts usage of surveillance-based teleworking technologies. This reveals the potential lack of and need for political and industrial sociologists[4] in policy development. Moreover, it is notable that Canada's policy will

[4] Industrial sociology can be defined as "the direction and implications of trends in technological change, globalisation, labour markets, work organisation, managerial practices and employment relations; the extent to which

require the individual responsible for the operation of AI to identify and mitigate the risks of harm or biased output (*Bill C-27*, 2022) whereas Greece's policy approaches the prevention of bias.

5.1.2 The Collection of Personal Data

The Consumer Privacy Protection Act intends on prompting the concept of proportionality, articulating that intrusive measures taken with respect to the collection of data must be proportional to the reason, thus, must be for reasonable purposes and out of legitimate organizational necessity (*Bill C-27,* 2022). Yet, it does not apply to the collection and use of personal information for purposes related to communication or for the facilitation of communication. Here, it is important to highlight that this articulation is vague, as it lacks specificity and clarity in defining what constitutes a legitimate organizational necessity. The term legitimate can be subjective and open to interpretation. Without the establishment of clear guidelines or criteria for determining necessity, this poses a risk of inconsistency in its application, rendering uniformity and accountability in both data collection and privacy practices difficult to achieve. When discussing legitimacy in the context of data collection, a clear guideline, or criteria to determine what constitutes as a necessity is essential. An insufficient illustration of what legitimacy encompasses poses a risk of inconsistency in how it is applied and, in turn, holds a significant potential to lead to varying standards and lack of uniformity with data collection practices, a situation that can be identified currently. Restricting the scope of the Act for the purpose of communication, without a comprehensive depiction of what this entails,

---

these trends are intimately related to changing patterns of inequality in modern societies and to the changing experiences of individuals and families; and the ways in which workers challenge, resist and make their own contributions to the patterning of work and shaping of work institutions." (Watson, 2011, p.1)

may also render it challenging to identify, consequently impeding on the implementability of the remaining provisions of the Act. This further signifies a potential gap between the policy's objective and its ability to be mobilized at the level of the individual. From the Foucauldian lens, the use of security power can be identified through the governance of an abstract entity and the detachment from individual peoples' realities. The guidelines offered by the HDPA, rather, articulates explicit examples of what is to be considered an intrusive measure, including the use of AI software or any other use of technology requiring the employee to preform regular action to prove their presence behind the screen (HDPA, 2021). Moreover, the HDPA approached the concept of legitimate use of this form of data collection quite differently, determining that the continuous surveillance of this nature is highly unlikely to be proportionate to its purpose. The Consumer Privacy Protection Act has also permitted the use of AI within organizations for decision-making purposes, on the condition that the organization makes information available on account of its general use (*Bill C-27*, 2022). This indicates an acknowledgement to potential benefits and efficiencies the use of AI can bring to business operations, however, must be used for justifiable purposes. Along with permitting the collection of data with reason, this furthers the abstraction of what the entity under governance truly is, thus presenting hurdles to its implementation in practice. The establishment of clear and concise guidelines and criteria would enable governance over phenomena with concrete existence.

Here, it should be pointed out that the transition to telework has led to an increase in online activities and time spent online, resulting in expansion of individuals' digital footprints (Haider and Anwar, 2023), being one of the leading sources of increased data transmission over the Internet since the pandemic (Sapenta and O'Brien, 2023). As the vast majority of the additional Internet usage is a result of telework, the limited regulation of surveillance

technologies can be consequential. Privacy policies for the software predominantly address the storing of information, of which varies depending on the software in question. This too, varies depending on the software. For instance, the WorkTime software collects information through a cloud-based service, and though collects intrusive data, such as “when the computer is actively used”; “active application, document and url”; and “applications currently being worked on, web URLs visited, time you are active, whether your mouse is actively moving or not, the amount of time worked on each app/document, the browser version you are using”, are stored on CoreSite servers (WorkTime Privacy Policy, 2023, pp. 8). CoreSite operates according to the industry best practices with respect to data collection, governed by “the highest standard of ethics” and “disciplinary protocols” (CoreSite Governance, 2023, pp.2). CoreSite also requires their employees to undergo an annual ethics training, of which includes acknowledgement and acceptance of the code of conduct and provides their cloud-service operating employees with a whistleblowing policy (CoreSite Governance, 2023). In comparison, Clockify’s (2023) privacy policy indicates that “personal data that is collected and processed by COING Inc.” (pp.2). As Clockify’s data processor, COING, “determines the purposes and the essential means of the processing of personal data” (Clockify Privacy Policy, 2023, pp. 15). COING, with an office in California (Clockify Privacy Policy, 2013) is headquartered in Serbia (COING, 2023), does not have a privacy policy on their webpage, with its operations described under its partners’ privacy policy. Accountability for code of conduct lies with software developers and operators, and though the OPC (2012) cautions developers of malware when using development kits, this accountability and caution has not yet been explicitly announced to private sector organizations with the use of software for telework. In addition to underlining the decrease in privacy recommendations from the OPC accepted across organizations since the mass shift to

teleworking, (OPC Departmental Plans and Departmental Results Report, 2022), it is also recognized that these recommendations are discretionary in terms of implementation. With the developments in the Digital Charter, organizations are only responsible for the information under their control and face limited restrictions with regard to the use of AI and the collection and use of information, it renders the policies with minimal tools for its implementation. The issue of accountability is not limited to intentional exploitation of ambiguity, but also weakens a given organization's responsibility to ensure the software programs used for teleworking possess a well-founded security and privacy policy, especially in cases where the organizations require the employees to utilize personal devices for work. The lack of well-defined guidelines poses issues with regard to accountability, enabling data collectors and processers the ability to exploit the ambiguity and continue to engage in practices that may neglect privacy and ethical standards that the Bill intends to establish in order to maximize productivity and enhance economic performance.

5.2 Concluding Remarks

The cross-case analysis demonstrated key differences in Canada's and Greece's approach to regulating the increasingly digitized arena. As opposed to Greece, which has shown to have deviated from wholeheartedly adopting the philosophy, Canada's profound adoption to a neoliberal governance paradigm has led to an approach to regulation of technologies and implementation of security measures that centers economic rationality and thus cautiously avoids potential hindrances to economic efficiency and productivity. It has demonstrated great mobilization of security power, in that the Bill has deliberately been formulated to refrain from imposition of overly restrictive measures, absenting precision by design. The formulation of the

Bill, as opposed to that of Greece, facilitates disciplinary power on the organizational level as the use of surveillance and monitoring technologies in private sector working practices have not been explicitly addressed. The execution of security power through the governance of an ambiguous issue devolves the matter of compliance to private sector organizations, enabling the use of disciplinary power over individuals to safeguard self-regulating behaviours.

Conclusion and Discussion

In carrying out a cross-case analysis, the Canadian case has demonstrated a strong commitment to market-oriented principles and attempted to minimize imposing barriers to movement of economic activities. Although the future of work and labour were the fundamental drivers behind the formulation of the Digital Charter, the specific inclusion of remote work was noticeably absent in addition to the regulations surrounding organizational operations being open-ended. The dominance of the neoliberal governmentality is persistent with the developments of the Digital Charter, showcased in the Charter's apprehensions to impose excessively stringent regulations, rendering the formulation of the Digital Charter to be a case in point with respect to security power, in addition to perpetuating the use of disciplinary power within private sector organizations. Though Greece is also a neoliberal state, it has long showed resistance in adopting neoliberalism, and still demonstrates reluctance in adopting it as a core, principle-driving ideology in policymaking. This paper argues that it is for this reason, that the HDPA's approach to policy has not instilled market-bolstering at the center of its decisions. In contrast, the framework has centralized social and ethical principles of the individual. The HDPA has put forth pronounced restrictions on disciplinary power, and, in doing so, has produced an un-ambiguous legal framework. Neoliberalism exacerbates job insecurity to stimulate competition and productivity. The rise of telework in the post Covid-19 era has resulted in a significant increase in online presence, in turn, being the leading factor for the demand and utilization of surveillance technology, such as surveillance and monitoring software. This has perpetuated power imbalances within workplaces, disallowing workers from expressing worry, discomfort, or leaving them fearing portraying incompetence. Fear of losing employment or damaging reputation has played a disciplinary role in indirect coercion and compliance to adopting

teleworking practices. Despite the developments made to *Bill C-27*, the Acts, and thus policies under the Bill, have not offered sufficiently significant or concrete regulatory guidelines applicable at the level of the individual worker. Organizational operations within the private sector will likely not achieve considerable standardization as a result of Digital Charter, as the neoliberal paradigm under which it was created has approached the development of the Bill with exercising security power. The use of security power, and thus the absence of a concrete governance over the digital arena, not only leaves the market for surveillance technologies unregulated, but also facilitates the economic objective behind neoliberal labour market policies through enabling disciplinary power on a micro scale, and thus at the level of the individual. The use of security power has shown to enable the absence of concrete oversight over the teleworking labour force, resulting in minimal progression with respect to privacy and security as the market for surveillance technologies remains marginally regulated. Greece has exhibited a notable shift from a firm neoliberal approach in the regulation of surveillance tools employed within the private sector labour market. The teleworking framework established by the HDPA implements guidelines using a top-down approach, delineated what constitutes as intrusive measures, and emphasizes that said measures are unlikely to be justifiably used. In articulating the boundaries, limitations, and accountability of the data controller, the HDPA framework aims to safeguard the privacy and security rights of teleworking individuals and denies employers the right to utilize systems requiring employees to demonstrate their presence behind the screen. As demonstrated throughout, this is an area heavily relied upon by private sector employers in Canada and remains without oversight. As organizations are only accountable for the information they can control, this leaves a lack of answerability should the unregulated software collect information without consent or introduce malware or spyware on one's device. This study

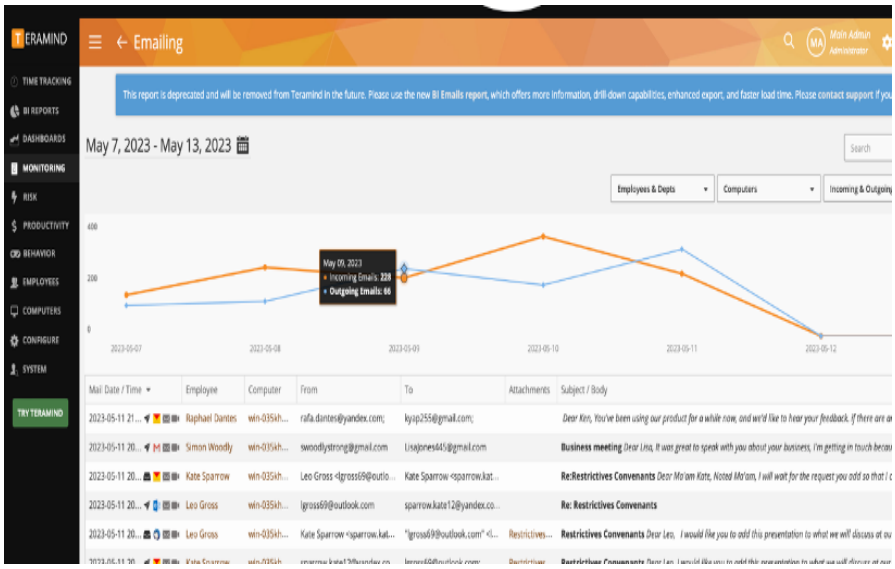
has highlighted the implications of neoliberal governance paradigm and its policy developments made on privacy and security in the digital arena within the Canadian context. The neoliberal governance paradigm, with its emphasis on deregulation and market-driven approaches, has led to potential harmful vulnerabilities. The prioritization of market forces and individual autonomy has overshadowed the establishment of robust security measures. Moreover, with the consultation taking place prior to the Covid-19 pandemic, with the primary topics of discussion orbiting around the subject of the future of work, the developments to the Digital Charter are peripheral. The neoliberal governance paradigm has substantially guided the course of action undertaken by the Government of Canada. It has preserved the neoliberal overarching objective of maximizing macroeconomic performance, despite the Bill's aim to provide protection of individuals and individuals' personal information, thereby resulting in a lack of well-defined guidelines and criteria. The Foucauldian conceptual framework unveils the approach undertaken, in that the Bill demonstrates the use of security power by attempting to implement a degree of control without the use of definitiveness or decisiveness, thereby enabling minimizing imposing hindrances to economic performance and further enabling the use of disciplinary techniques carried out internally within private sector organizations. With consideration to the evolving nature of work and the increasing reliance on technology, there is a growing urgency to reassess the framework of governance pertaining to the digitalization of Canada, and principally on the digitalization of work. The deep-rooted neoliberal governmentality has rendered the Bill insubstantial in addressing privacy and security issues with respect to the future of work, granted the lack of clearly stated or decided guidelines necessary practical implementation. As Greece's economic system has adopted neoliberalism and does not substantially differ from that of Canada's, its approach to regulation over telework serves great insight. It demonstrates the

capacity to strike balance between operating a neoliberal economic system and safeguarding its citizens by interdicting exploitative practices. This study has highlighted the importance of evaluating current governance strategies and approaches, particularly in an era defined by technological innovation and digital labour markets. Furthermore, it underscores the critical role of public administration and the importance of evaluating the suitability of broader policy frameworks in policy development and implementation, in order to ensure alignment with the evolving needs of society.

Future research should consider expanding this case study by examining the temporal success and assessing the efficacy of the HDPA's policies in practice. Moreover, using this research paper as a point of departure, further Canadian research on different workplaces, the industry, the demographic employed, and the software per profession to gather information on the potential impacts of non-standardized telework on different occupational demographics would offer valuable depth to the study of Canadian public administration in the scope of digital policy implementation. As the National Digital and Data Consultation was predominantly led by individuals with entrepreneurial orientation, diversification by way of a sociological approach may be valuable in acquiring information on more at-risk social groups or industries and assessing the ways in which the new forms, requirements, and conditions of work in the digital sphere may contribute to systemic and/or systematic inequalities.

Figure 1:

Example of email monitoring feature from Teramind software



Note: An example of the inbound and outbound email monitoring feature displayed on the Teramind website for promotional purposes.

References

Abulibdeh, A (2020). Can COVID-19 Mitigation Measures Promote Telework Practices? *Journal of Labor and Society* 23 (4): 551–76.

Adams-Prassl, J. (2019). *What if Your Boss Was an Algorithm?* The Rise of Artificial Intelligence at Work. *Comparative Labor Law & Policy Journal* 4(1) 123, https://ssrn.com/abstract=3661151

Allen, R, QC. & Masters, D. (2021). Technology Managing People- the legal implications. *Trades Union Congress. Retrieved from https://www.tuc.org.uk/sites/default/files/Technology_Managing_People_2021_Report_AW_0.pdf*

Aloisi, A. and De Stefano, V. (2022), Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. International Labour Review, 161: 289-314. https://doi.org/10.1111/ilr.12219

Anaya, T. (2022). *Workplace surveillance: Employee monitoring stats in Canada. Capterra.* https://www.capterra.ca/blog/2733/workplace-surveillance-employee-monitoring-software

Asana. (2023). *Manage your team's work, projects, & tasks online*. Asana. https://asana.com/

Azar, E. E., & Farah, N. (1981). The structure of inequalities and protracted social conflict: A theoretical framework. International Interactions, 7(4), 317–335. https://doi.org/10.1080/03050628108434558

Ball, K. (2010). Workplace surveillance: an overview, Labor History, 51:1, 87-106, DOI: 10.1080/00236561003654776

Bérastégui, P. (2021). Teleworking in the aftermath of the Covid-19 pandemic. The *European Trade Union Institute*. Retrieved from https://www.etui.org/publications/teleworking-aftermath-covid-19-pandemic

Bill C-27 (2022): An act to enact the consumer privacy protection act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and data act and to make consequential and related amendments to other acts: Digital Charter Implementation Act.

Capterra. (n.d.). Employee monitoring software. *Capterra.* https://www.capterra.ca/directory/31087/employee-monitoring/software?countries%5B%5D=CA&amp%3Bsort=popularity

Carroll, L. (2022). *Driving a culture of innovation with Ontario's Public Service*. Microsoft Industry Blogs - Canada. https://www.microsoft.com/en-

ca/industry/blog/government/2022/04/29/driving-a-culture-of-innovation-with-ontarios-public-service/

Catană, Ș.-A., Toma, S.-G., Imbrișcă, C., & Burcea, M. (2022). Teleworking Impact on Wellbeing and Productivity: A Cluster Analysis of the Romanian Graduate Employees. Frontiers in Psychology, 13, 856196–856196. https://doi.org/10.3389/fpsyg.2022.856196

Cawley, R. M., & Chaloupka, W. (1997). American Governmentality: Michel Foucault and Public Administration. American Behavioral Scientist, 41(1), 28–42. https://doi.org/10.1177/0002764297041001004Chawla, A. (2021). Pegasus Spyware – 'A Privacy Killer'. 1- 9.http://dx.doi.org/10.2139/ssrn.3890657

Chenou, J.-M. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. Globalizations, 11(2), 205–223. https://doi.org/10.1080/14747731.2014.887387

Clark, D. (2002). Neoliberalism and Public Service Reform: Canada in Comparative Perspective. *Canadian Journal of Political Science / Revue Canadienne de Science Politique*, *35*(4), 771–793. http://www.jstor.org/stable/3233289

Connecteam. (2022). All-in-one free GPS tracker app. https://lp.connecteam.com/employee-monitoring-app-aw/?utm_source=capterra.com&utm_medium=cpc&utm_campaign=employee-monitoring&utm_adgroupname=capterra

CoreSite. (2023). Governance. CoreSite: An American Tower Company. https://www.coresite.com/about/governance

CurrentWare. (2023). Real-Time Employee Monitoring Software for Workforce Productivity *CurrentWare*. https://www.currentware.com/products/browsereporter/?utm_source=capterra

Clary, W. G. (2022). Surveillance of Teleworkers: A Grounded Theory Approach. ProQuest Dissertations Publishing.

Crain, M. (2021). THE PRIVACY CHALLENGE. In *Profit over Privacy: How Surveillance Advertising Conquered the Internet* (pp. 113–134). University of Minnesota Press. https://doi.org/10.5749/j.ctv20zbktm.9

Deibert, R. (2022). Protecting Society from Surveillance Spyware. *Issues in Science and Technology*, 38(2), 15–17. Retrieved from https://login.proxy.bib.uottawa.ca/login?url=https://www.proquest.com/scholarly-journals/protecting-society-surveillance-spyware/docview/2693960397/se-2

Delfanti, A., & Frey, B. (2020). Humanly Extended Automation or the Future of Work Seen through Amazon Patents. Science Technology and Human Values. Scopus. https://doi.org/10.1177/0162243920943665

Dolowitz, D.P. and Marsh, D. (2000) Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making. Governance, 13, 5-24. http://dx.doi.org/10.1111/0952-1895.0012

Elden, S. (2007). Governmentality, Calculation, Territory. Environment and Planning. D, Society & Space, 25(3), 562–580. https://doi.org/10.1068/d428t

European Parliament. (2023). Study: The impact of Pegasus on fundamental rights and democratic practices. *Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies.* PE 740.524.

EU Reporter Correspondent. (2022). Greek parliament approves spy operation reforms. Retrieved from https://www.eureporter.co/world/greece/2022/12/12/greek-parliament-approves-spy-operations-reforms/

Farmer, D. J. (1995). Kill the King: Foucault and Public Administration Theory. Administrative Theory & Praxis, 17(2), 78–83. http://www.jstor.org/stable/25611128

Fenton, N. (2011). Deregulation or democracy? New media, news, neoliberalism and the public interest, *Continuum*,25:1, 63-72,DOI: 10.1080/10304312.2011.539159

Foucault, M. (1975). Discipline and Punish – The Birth of the Prison, Vintage Books, New York: Pantheon.

Foucault, M. (1980). Power/Knowledge: Selected Interviews and Other Writings, 1972-79, (Ed. Colin Gordon). New York: Pantheon.

Foucault, M. (1975). Discipline and Punish – The Birth of the Prison, Vintage Books, New York: Pantheon.

Foucault, M. & Burchell, G. (2009). *Security, Territory, Population: Lectures at the Collège de France 1977-1978*. Translated by Graham Burchell. New York: Picador.

Foucault, M., Ewald, F., & Fontana, A. (2008). The birth of biopolitics: lectures at the Collège de France, 1978-79 (M. Senellart, Ed.; G. Burchell, Trans.). Palgrave Macmillan.

Fuchs, C. (2019). Karl Marx in the Age of Big Data Capitalism. In C. Fuchs & D. Chandler (Eds.), *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data* (pp. 53–72). University of Westminster Press. http://www.jstor.org/stable/j.ctvckq9qb.6

Gal, U., J T. B., & Stein, M.-K. (2020). Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. Information and Organization, 30(2), 100301–. https://doi.org/10.1016/j.infoandorg.2020.100301

Gane, N. (2001). Zygmunt Bauman: Liquid Modernity and Beyond [Review of *Liquid Modernity; The Individualized Society; The Bauman Reader*, by Z. Bauman, Z. Bauman, & P. Beilharz]. *Acta Sociologica*, *44*(3), 267–275. http://www.jstor.org/stable/4194889

Gane, N. (2012). The governmentalities of neoliberalism: panopticism, post-panopticism and beyond. *The Sociological Review (Keele)*, 60(4), 611–634. https://doi.org/10.1111/j.1467-954X.2012.02126.x

Garden,C (2018). Labor Organizing in the Age of Surveillance, *Seattle University School of Law Digital Commons. 63*(55), 55-68. https://digitalcommons.law.seattleu.edu/faculty/814

George, J. F. (1996). Computer-Based Monitoring: Common Perceptions and Empirical Results. MIS Quarterly, 20(4), 459–480. https://doi.org/10.2307/249564

Gill, J. K. (2021). Unpacking the Role of Neoliberalism on the Politics of Poverty Reduction Policies in Ontario, Canada: A Descriptive Case Study and Critical Analysis. *Social Sciences*, *10*(12), 485. https://doi.org/10.3390/socsci10120485

Gillis, A. S. (2022, March 4). *What is IOT (internet of things) and how does it work? - definition from techtarget.com*. IoT Agenda. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Gönenç, D., & Durmaz, G. (2020). The politics of neoliberal transformation on the periphery: a critical comparison of Greece and Turkey. Journal of Southeast European and Black Sea Studies, 20(4), 617–640. https://doi.org/10.1080/14683857.2020.1843284

Government of Canada. (2019). *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*. Government of Canada. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/canadas-digital-and-data-strategy

Government of Canada. (2022). GC Infobase - open datasets - departmental plans and departmental results reports – performance information by program and by organization. *Open Government Portal.* https://open.canada.ca/data/en/dataset/a35cf382-690c-4221-a971-cf0fd189a46f/resource/09c15494-788e-4991-ad00-2bd905c4f225

Graham, S., & Wood, D. (2003). Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy*, *23*(2), 227–248. https://doi.org/10.1177/0261018303023002006

Greece Ministry of Justice ("ΥΠΟΥΡΓΕΙΟ ΔΙΚΑΙΟΣΥΝΗΣ"). (2022). *Completion of public electronic consultation on the draft law under the title: "Procedure of privacy of*

communications, cyber security and protection of citizens' personal data". http://www.opengov.gr/ministryofjustice/?p=16477

Hall, P.A. (1993). Policy paradigms, social learning, and the state: The case of economic policymaking in Britain. *Comparative Politics* 25 (3): 275-295

Haider, M. and Anwar, A.I. (2023), "The prevalence of telework under Covid-19 in Canada", *Information Technology & People*, Vol. 36 No. 1, pp. 196-223. https://doi.org/10.1108/ITP-08-2021-0585

Hellenic Data Protection Authority. (2021) GUIDELINES 1/2021 Regarding the application of personal data protection rules in the context of telework, 1–14. Retrieved from https://www.dpa.gr/sites/default/files/2021-08/Katefthintiries_grammes_1_2021.pdf

Henman, P. (1997). Computer Technology – a Political Player in Social Policy Processes. Journal of Social Policy, 26(3), 323-340. doi:10.1017/S0047279497005035

Hofmeyr, B. (2022). Foucault and governmentality: living to work in the age of control. Rowman & Littlefield.

House of Commons Canada. (2022). (rep.). *DEVICE INVESTIGATIVE TOOLS USED BY THE ROYAL CANADIAN MOUNTED POLICE AND RELATED ISSUES* (pp. 1–42).

House of Commons Canada. (n.d.). Welcome to the House of Commons of Canada - House of Commons of Canada. https://www.ourcommons.ca/en

Industrial Relations and Labour Law (2021). Greece: Greek Law 4808/2021 - Major reforms in employment legislation. Retrieved from https://industrialrelationsnews.ioe-emp.org/industrial-relations-and-labour-law-august-2021-1/news/article/greece-greek-law-4808-2021-major-reforms-in-employment-legislation

Jackson, A., & Thomas, M. P. (2017) *Work and Labour in Canada: Critical Issues*. Toronto, Ontario: Canadian Scholars

Kaster, S. D., & Ensign, P. C. (2023). Privatized espionage: NSO Group Technologies and its Pegasus spyware. Thunderbird International Business Review, 65(3), 355–364. https://doi.org/10.1002/tie.22321

Keeley, J. F. (1990). Toward a Foucauldian Analysis of International Regimes. *International Organization*, *44*(1), 83–105. http://www.jstor.org/stable/2706810

Kennedy, G. (2016). Embedding neoliberalism in Greece: the transformation of collective bargaining and labour market policy in Greece during the Eurozone crisis. Studies in Political Economy, 97(3), 253–269. https://doi.org/10.1080/07078552.2016.1249129

King, A. G., & Mrkonich, M. J. (2016). Big data and the risk of employment discrimination. *Oklahoma Law Review, 68(3),* 555-584.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear Phishing emails? *Telematics and Informatics,* 48, 101343– https://doi.org/10.1016/j.tele.2020.101343

Lally, L. (1996). Privacy versus Accessibility: The Impact of Situationally Conditioned Belief. Journal of Business Ethics, 15(11), 1221-1226. Retrieved from http://www.jstor.org.ezproxy.library.yorku.ca/stable/25072846

Leiner, M.B., Cerf, G.V., Clark, D.D., Kahn, E. R., Kleinrock, L., Lynch, D. C. Postel, J., Roberts, G. L. & Wolff, S. (1997). A Brief History on the Internet. *Internet Society. https://www.internetsociety.org/internet/history-internet/brief-history-internet/*

Leonidas, M. (2022). *The benefits of tapping into cloud processing power*. NIC IT Solutions. https://www.nicitpartner.com/benefits-tapping-cloud-processing-power/#:~:text=Cloud%20processing%20power%20offers%20your,servers%20at%20different%20physical%20locations

Lowe, Graham S. (2002). Employment Relationships as the Centrepiece of a New Labour Policy Paradigm. *Canadian Public Policy / Analyse de Politiques* 28 (1): 93–104. https://doi.org/10.2307/3552163

MacKinnon, S. (2011).The Effectiveness of Neo-Liberal Labour Market Policy as a Response to the Poverty and Social Exclusion of Aboriginal Second-Chance Learners. *Library and Archives Canada* 1-307.

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. Surveillance & Society. 16. 219-237. 10.24908/ss.v16i2.8346.

Manokha, I. (2020). Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic, Political Anthropological Research on International Social Sciences (PARISS), 1(2), 273-287. doi: https://doi.org/10.1163/25903276-BJA10009

Masoodi, M.J., Abdelaal, N., Tran, S., Stevens, Y., Andrey, S. and Bardeesy, K. (2021).*Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada.* Retrieved from https://www.cybersecurepolicy.ca/workplace-surveillance

Mcbride, S., & Mcnutt, K. (2007). Devolution and Neoliberalism in the Canadian Welfare State: Ideology, National and International Conditioning Frameworks, and Policy Change in British Columbia. Global Social Policy, 7(2), 177–201. https://doi.org/10.1177/1468018107078161

McNicoll, G. (2007). [Review of *Security, Territory, Population: Lectures at the Collège de*

France, 1977-78, by M. Foucault]. *Population and Development Review*, *33*(4), 829–831. http://www.jstor.org/stable/25487628

Microsoft. (2022). Hybrid work is just work: are we doing it wrong? *Work Trend Index Special Report.* Retrieved from https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work-is-just-work

Microsoft Security. (2023). *What is malware?: Microsoft security*. What Is Malware? | Microsoft Security. https://www.microsoft.com/en-ww/security/business/security-101/what-is-malware#:~:text=Spyware,settings%2C%20and%20decrease%20device%20performance.

Migliano, S. (2023). Report: Employee Monitoring Software Demand Trends 2020-23. Privacy risks of employee monitoring software. https://www.top10vpn.com/research/covid-employee-surveillance/

Mouratidis, K., & Papagiannakis, A. (2021). COVID-19, internet, and mobility: The rise of telework, telehealth, e-learning, and e-shopping. *Sustainable cities and society*, *74*, 103182. https://doi.org/10.1016/j.scs.2021.103182

Noble, S. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York, USA: New York University Press. https://doi.org/10.18574/nyu/9781479833641.001.0001

Office of the Privacy Commissioner of Canada. (2019). *Pipeda in brief*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#

Personal Information Protection and Electronic Documents Act, SC 2000 c. 5

Petrosyan, A. (2023). Cyber attacks in organizations global 2022. *Statista.* https://www.statista.com/statistics/1376249/cyber-attack-global-firms-by-type/

Pupo, N & Duffy, A. (2012). Unpaid work, capital and coercion. *Work Organisation, Labour & Globalisation*, *6*(1), 27–47. https://doi.org/10.13169/workorgalaboglob.6.1.0027

Pupo, N., Duffy, A, & Glenday, D. (2017). *Crises in Canadian Work: A Critical Sociological Perspective.* Don Mills, Ontario, Canada: Oxford UP.

Randstad. (2023) Is work from home the future? | *Randstad Canada.* https://www.randstad.ca/job-seeker/career-resources/work-from-home/work-from-home-future/

Robins, K. & Webster, F. (1993). "I'LL BE WATCHING YOU": COMMENT ON SEWELL AND WILKINSON. Sociology, 27(2), 243–252. http://www.jstor.org/stable/42855174

Robins, K., & Webster, F. (1999). Times of the technoculture : from the information society to the virtual life. Routledge. https://doi.org/10.4324/9780203169544

Sargiacomo, M. (2009). Michel Foucault, Discipline and Punish: The Birth of the Prison: Allen Lane, London, 1977, Trans. by Alan Sheridan. *Journal of Management & Governance*, *13*(3), 269–280. https://doi.org/10.1007/s10997-008-9080-7Shaw, N. (2022). Spyware: the rise of sextortion. *Always Networks Ltd* . Retrieved from https://alwaysnetworks.co.uk/spyware-the-rise-of-sextortion/.

Schiller, D. (1999). Digital capitalism: networking the global market system. MIT Press.

Sepanta, F., & O'Brien, W. (2023). Review and exploration of relationships between domains impacted by telework: A glimpse into the energy and sustainability considerations, COVID-19 implications, and future research. Renewable & Sustainable Energy Reviews, 183. https://doi.org/10.1016/j.rser.2023.113464

Shore, J.B .(1999). Teleworking: A Fact Sheet. Office of Governmentwide Policy. Archive.*USA Gov. https://govinfo.library.unt.edu/accessamerica/docs/Telecommfact.html*

Skype. (2023). Can I monitor a member's usage with Skype manager? Skype Support. https://support.skype.com/en/faq/FA561/can-i-monitor-a-member-s-usage-with-skype-manager

Sládek, P., & Sigmund, T. (2021). Legal Issues of Teleworking. SHS Web of Conferences, 90, 1020–. https://doi.org/10.1051/shsconf/20219001020

Spanou, C. (2020). Public Administration. In The Oxford Handbook of Modern Greek Politics. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198825104.013.11

Taekke, J. (2011). Digital Panopticism and Organizational Power. *Surveillance & Society*,8 (4): 441–54. 10.24908/ss.v8i4.4181

Teramind Inc. (2023). *Email monitoring*. Teramind. https://democompany.teramind.co/#/reports/emailing

Time Doctor . (n.d.). Employee Time Tracking with Time doctor. S*imple and Accurate Time Tracking with Time Doctor* | Time Doctor. https://www.timedoctor.com/employee-time-tracking?utm_medium=cpc&utm_source=google&utm_campaign=Brand-T1-AU-UK-CA

Thiel, S. van. (2014). Research methods in public administration and public management : an introduction. Routledge.

Thormundsson, B. (2023). Topic: Artificial intelligence (AI) adoption, risks, and challenges. *Statista*.https://www.statista.com/topics/10548/artificial-intelligence-ai-adoption-risks-and-challenges/#topicOverview

Togman, R. (2021). Foucauldian security and the threat to democratic policy-making. *Critical Review of International Social and Political Philosophy*, *24*(2), 230–252. https://doi.org/10.1080/13698230.2018.1535734

Tong, G. C. (2023). Employee surveillance is on the rise - and that could backfire on employers. *CNBC.* https://www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html

Törnberg, P. & Justus, U. (2020). Complex Control and the Governmentality of Digital Platforms. *Frontiers in Sustainable Cities*, 2,(6): 1–11.https://doi.org/10.3389/frsc.2020.00006

Traqq. (2023). *Time Tracker for teams and individuals*. Traqq. https://traqq.com/

Trudeau, G. (2002). Changing Employment Relationships and the Unintentional Evolution of Canadian Labour Relations Policy. *Canadian Public Policy / Analyse de Politiques* 28 12

U.S. Congress, Office of Technology Assessment, The Electronic Supervisor: New Technology, New Tensions, OTA-CIT-333 (Washington, DC: U.S. Government Print- ing Office, September 1987).

Watson, T. (2011). Sociology, Work and Organisation: Seventh Edition (6th ed.). Routledge. https://doi.org/10.4324/9780203805268

WorkTime.(2023). Privacy policy. WorkTime. https://www.worktime.com/privacy-policy

Yin, R. K. (2017). Case Study Research and Applications, 6th Edition. [VitalSource Bookshelf 10.3.3]. Retrieved from vbk://9781506336176

Yang, R.J & Liu, J. (2023). Strengthening accountability for discrimination: Confronting fundamental power imbalances in the employment relationship. *Economic Policy Institute.* 1-53. Retrieved from epi.org/218473

Zureik, E. (2020). Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel. Middle East Critique, 29(2), 219–235. https://doi.org/10.1080/19436149.2020.1732043