THESIS MBA 2023

Research Question

Does employee monitoring infringe on workers' right to privacy, while working from home?

Word count excluding abstract and references: 13,478

Submitted By

Elizabeth O'Connell

August 2024

Student ID Number: 21138915

X21138915@student.ncirl.ie

Acknowledgments

Professor Paul Hanly. Thesis Supervisor

MBA Lecturers. Class of 2021 to 2023

Academic Operations

MBA Class of 2021 to 2023

Mr Keith Brittle. NCI Librarian

Survey Research Respondents

Professor Paul Hanly

Paul, as my thesis supervisor, thank you for your unwavering support. Especially when I needed to defer my thesis submission until 2024. Thanks also for reminding me on several occasions to decant the knowledge learned during the course, from my brain onto the research paper!

MBA Lecturers. Class of 2021 to 2023

To you all, many thanks for imparting your knowledge and experience. It was very much appreciated. Hard task masters at times, but well worth it. Thanks also for your guidance completing course work.

Academic Operations

Many thanks to this office. The people within, often go unnoticed as being instrumental in the smooth running of operations. Particular mention to Ms Priscila Flora Reis for her kindness and support navigating the deferral process and resolving technical issues.

MBA Class of 2021 to 2023

What can I say, a fabulous bunch of classmates. Their friendship and support were appreciated through out the two years. The opportunity to interact with others during Covid lockdowns was challenging. But we managed to get to know one another pretty well overall. As MBA Class Rep for both years 2021 to 2023, they made this position a positive and rewarding experience.

Mr Keith Brittle. NCI Librarian

Keith your guidance on prepping my thesis was a valuable insight.

Survey Research Respondents

Grateful thanks to all who took the time to participate in my survey, to support the research. Without which, it would have made the process extremely difficult. Unfortunately, due to ethics and anonymity requirements, you will remain forever the unsung heroes of my thesis.

Abstract

The study investigated the impact of monitoring on the privacy of a remote worker in the home. Pre Covid a considerable portion of remote working was the preserve of Gig workers of the Gig economy. It was more often than not a lifestyle choice due to the flexibility. The Covid 19 Pandemic thrust a considerable portion of the workforce into unchartered territory at an extraordinary and unexpected pace. The preservation of an organisation, its survival and that of its employees required changes to day-to-day operations. The prolific use of monitoring technology was implemented. Little consideration was given to the balance between trust and control or the potential imbalance of a power dynamic. This research proposal explores the advantages and disadvantages of remote worker tracking through the use of monitoring technology, IoT and AI. Given the rapid pace of advancements in tracking technology capabilities, we currently reside within the era of artificial intelligence to deliver services. In order to effectively serve the interests of all stakeholders involved, it becomes imperative to foster progress in remote worker technology parameters in terms of privacy.

The survey data was collected from 26 participants using a Microsoft Survey Forms. There are three very important considerations where technology is used to monitor employees in their home environment. (a) Does the use of technology in the digital era impact on a worker's right to privacy at home, (b) Does an employee know or understand the type of technology being used to monitor them off site, (c) Does the employee know the type of data collected and what the data will be used for?

The research examined survey responses and established a link between the way in which digital monitoring technology was viewed by an employee and the lack of transparency within organisations using such technology. It is unclear whether organisations are passively collecting data, with no clear intention of use or there is an underlying agenda to use harvested data as a measure of control against employees. The focus of the research was assisted by the thematic analysis of the data in addition to peer-reviewed journal research. By examining the potential benefits and challenges associated with worker tracking, the research provides an analysis of its efficacy, ethical considerations, impact on organizational productivity, and whether such technology is an invasion of a worker's right and expectation to privacy. Remote working remains an integral part of an organisation, where practical post Covid. The right of a worker or indeed an employer to include remote or hybrid working as part of employment has forced adaptation within organisations.

Table of Contents

Methodology

1. Research Collection Methodology
2. Data Collection and Sampling Criteria
3. Survey Questions
4. Data Collection Method
5. Research Limitations
6. Future Research Scope
7. Survey Data Analysis
8. Research Methodology Discussion

Introduction

Does employee monitoring infringe on workers' right to privacy while working from home?

The phrase "with great power, comes great responsibility". Its origins rooted as far back as the French Revolution, and the French author Voltaire. The quotation has been stated and paraphrased by Politicians, Prime Ministers and Presidents during the 20th Century. However, the essence of this coined phrase has never been more relevant in the 21st Century. The emergence of AI technology is a force to be reckoned with and society has an obligation and responsibility to ensure its ethical use for the greater good. This sentiment is very relevant to the use of high-tech AI driven surveillance monitoring of the working from home labour force. The purpose of this paper is to establish whether or not there is an impact on a worker's privacy while working from home.

Covid 19 was a catalyst to normalising remote and hybrid working. Beyond a desperate need on the part of the employer and employee to maintain a functioning entity from the onset of lockdown. There was little thought to the privacy aspect for a worker during lockdown and the "new" status quo, (Harvard Business Review *et al.* 2022)[44].

The purpose of this research is to identify existing weaknesses and potential weaknesses in a remote working environment for a worker's right to privacy. Heretofore, remote working (from home) was in the main a lifestyle choice and any infringement of worker's rights was an informed choice, (Kaduk et al., 2019)[52]**.** Research into remote working in general isn't new and many papers are available, for example, (Wolf, 2010)[111]. However, workers privacy is encompassed in the broader research on negative impacts rather than as a specific weakness or threat to workers' rights, (Galanti et al., 2023)[38].

The thesis will investigate the potential infringement of workers' right to privacy during working time and out of working hours due to the use of remote lone worker tracking

technology in the home. The right to disconnect has also attracted much attention in terms of burnout and a balance between work periods and rest periods. There is a concentration on workers' rights in terms of the use of technology to contact a worker or the "always on" challenge versus the right to disconnect, (Urbane, 2023)[106]. While separation of working time and rest time evaluation is important, once again there is little evidence of addressing a worker's right to privacy. Where a right to disconnect is employed, does that involve unplugging or switching off either hardware supplied or just ignoring an employer's request "out of hours". It does not address the fact that most IoT and AI have the capability to be in a constant state of monitoring. How the use of AI and IoT is managed fairly is a challenge and requires openness, fairness and governance, (Fares, Nedeljkovic and Jammal, 2023)[36]. The use of employee tracking historically tracked the worker in the workplace as an attendance or performance tool, or at a remote location for safety reasons. Now the lines of legitimate use have become blurred in so far as separating work environments from nonwork hours in what is predominantly a home environment occupied by family, friends and house mates, (Das Swain et al., 2020)[24].

Does the use of tracking technology under the banner of worker safety and or performance management also protect the privacy rights of the employee beyond the technology's stated purpose? The implications of the use of remote worker tracking have far reaching consequences on the individual worker in terms of what the data collected might be used for or indeed an invasion of privacy of family or cohabitants in the home, (Hewitt, 2023)[46]. By examining the implications, benefits, and limitations of remote tracking systems, this research seeks to provide insights into the efficacy and viability of such technologies in ensuring the safety and well-being of remote workers.

Through a comprehensive analysis, the study aims to contribute to the existing body of knowledge regarding the use of remote worker tracking. The use of technology for the purposes of lone worker tracking has its roots in the research and development of existing applications used every day in metaverse applications (Zhang et al., 2022)[113]. Through a balanced assessment of the pros and cons, stakeholders can make informed decisions regarding the implementation of remote lone worker tracking systems. However, the pace of tracking technology is such that, do we as a society even know the questions we should be asking, in terms of protection for worker privacy and rights or the safeguards we need to implement for the future, ((Mark, 2023)[68]. While Covid 19 propelled workers into a remote scenario, there is

an appetite to maintain both remote and hybrid as a right. There is however a long way to go in reaching an ideal environment in terms of workers privacy rights, (Katsabian,2023)[53].

Literature Review

The focus of the research and literature review concentrated on five areas of importance for the work from home employee.

1. Emerging AI remote worker technology

2.Ethical use of remote tracking and surveillance information

3.Employees

4.Respecting privacy rights

5.Informed decision making

The research of a worker's right to privacy is not in itself a new topic. However, research information, scholarly articles and critical evaluation on privacy is generally encompassed in associated areas related to worker rights. Evidence of in-depth research related to a worker's right to privacy specifically in the home office seems sparse as a standalone and appears to be encompassed in research papers on worker wellbeing and work life balance.

There is of course quantitative research available to support the hypothesis that IoT is capable of privacy invasion in the workplace, (Princi and Krämer, 2019)[84]. However, when a private home becomes the workspace. The imbalance of power and control between an employer and employee still exists. The research does require greater levels of investigation on the impact of "the always on" technology. Which can be accessed by an employer or a third-party provider to the organisation. Hence the aim of the research question is to establish whether the impact of surveillance technology used to monitor in a home environment is an invasion of a worker's right to privacy in a work from home setting.

Research and theory published, demonstrate investigation into the right to work remotely or stress levels or mental health and wellbeing, and of course possible burnout. This thesis aims to identify how a worker's right to privacy is impacted while working from home. Prior research analysis extracted for this thesis was specifically relevant to workers privacy,

emerging AI technology, ethical use of tracking information, respecting privacy rights, informed decision making, and the relationship an employee has with remote tracking. The purpose of the research question is to gain a greater understanding of the impact on and the infringement of a worker's privacy rights. The research question asks: Does employee monitoring infringe on workers' right to privacy, while working from home?

Pre Covid, there was little concern for remote worker monitoring as it was predominantly a situation of choice in so far as the trade-off for a worker in the Gig economy was flexibility above a worker rights or threat to liberty, (Hickson, 2023)[47]. The Gig economy model also bypasses many of the normal responsibilities of an employer, (Duggan et al., 2019)[28]. It was also the case that the level of sophisticated technology available today in the form of IoT and AI, was not a consideration in the earlier part of the 2010's.

With an unprecedented growth in AI technology, the need to investigate and monitor the pros and cons of remote worker technology is important. In the context of the impact of artificial intelligence and machine learning, there is a need to design and implement these technologies in a responsible manner. Globally, interested parties have defined many sets of high-level AI ethics principles to support this vision, (Sanderson et al., 2024)[89] .As we navigate the popularity of remote working beyond Covid 19. There has been an increase in a developing research agenda, (Gifford, 2022)[39]. The ethical dilemma of employee monitoring onsite or indeed remotely pre Covid was already compromising to a worker's rights, (Yerby, 2013)[112].

The impact of performance management during Covid and post Covid remains a challenge for organisations and how they approach workforce strategies, (Göndöcs and Dörfler, 2021)[41]. The literature review examines ethical concerns of remote tracking as a key component. The significance of informed consent, the responsible handling of data, and the requirement of striking a balance between tracking for organisational needs and observing employee privacy rights, (Aloisi and De Stefano,2022)[2]**.** The need for remote tracking technology to be governed by ethical standards and rules. All of which have been previously researched as a potential infringement within an onsite location rather than a home office environment.

The research reviews existing literature on remote or lone worker tracking, with a specific focus on the investigation of infringement of an employee's right to privacy. Transparency in the use of the latest technology such as AI software as a lone worker tracking technology. The review will explore theoretical foundations, conceptual frameworks and empirical studies related to the use of technology in monitoring lone workers. This section will examine the

implications, benefits, limitations, and challenges of using remote worker surveillance technology. The research seeks to provide insight into the efficacy and viability of using technology such as IoT and AI lone worker tracking in an employee home and personal environments.

Already used as the best-in-class system to use for the purposes of health and safety in the workplace, does IoT and AI technology invade the privacy of personnel working from home. Through comprehensive analysis, the research will investigate technical constraints, data protection, and privacy issues, and potential bias which may be generated by AI algorithms. Research into employee monitoring is not new, but the complexity of the research agenda required is struggling to keep pace with technological advances. Research of employee performance monitoring identifies that unlike direct supervision, employers who for example use EPM, can track individual employees continuously, randomly, or intermittently; discreetly or intrusively; and with or without warning or consent, (Ravid et al., 2019)[85].

The shift of surveillance technologies from the onsite workplace into our homes used as remote workspaces, illustrates how the scale and precision of technology has adapted to the changing nature of operations. However, research suggests that workers right to privacy and potential harm does not enjoy the same considerations as extolled on benefits such as health and safety, (Bernhardt, Kresge and Suleiman, 2022)[8]. The level of research currently available is minimal in terms of the use of AI specifically in remote worker technology, (Morley,2022)[74]. However, this paper has provided peer-reviewed articles that evaluate remote lone-worker technology, (Charbonneau and Doberstein,2020)[19].

Legislation has not kept pace with the use of technology as a surveillance tool. Both GDPR legislation and European law are still rooted in an employee's right to privacy in an employer's onsite location. No one could have foreseen the effects of a pandemic on organisations or the workforce. Protection for the employee's privacy rights in law has not evolved with where, when and how we work today. Expectation of privacy within the home as a normal work environment is not reflected in legislation under GDPR or European legislation. There is an attempt by EU legislators to produce a white paper on the legal and civil liabilities of the owners of AI. The EU has identified shortcomings with regard to establishing product liability for AI products and harm they may cause under current product liability law, (Madiega, 2023)[67].

This legal situation magnifies the dilemma for workers' rights. When an employer uses or indeed abuses the use of AI technology or there is a system failure or privacy breach. Should this impact the privacy of the home worker. Who becomes liable for the invasion of privacy. The worker is not protected in law under product liability, and neither are they protected under employment law where there is an invasion of privacy while working from home. Judicial developments concentrate only on employee privacy within the workplace as a fundamental right while onsite, (Keane, 2018)[56]. For example, in Ireland according to government literature available to employers of remote workers on the website of The Department of Enterprise, Trade and Employment. The department merely offers guidance and an employer checklist as to how remote workers should be dealt with in terms of GDPR, health and safety, and employment conditions. Specifically, under the heading of employee privacy for remote workers, The Government Department responsible for trade and employment quotes "Currently, there is no specific legislation dealing with a right to privacy in the workplace. According to the WRC, the Data Protection Acts and GDPR Regulations should be observed in terms of an employees' privacy when working remotely. Guides on applying these Acts are linked in the section below on data protection. The WRC also indicate that an employees' right to privacy is balanced against the rights of the employer to protect the undertaking, its reputation, resources and equipment." (enterprise.gov.ie, n.d.)[35]. The potential to allow invasive technology, privacy concerns, governance and ethics to go unchecked because of the absence of suitable legislation is less than ideal in an age where advancements in AI is exponential. There is an expectation that employee rights including privacy is enshrined in law.

Review of existing research suggests many deficits in protecting workers right to privacy while working from home. A common thread throughout this literature review is a recognition that AI growth has remarkable capabilities. However, such exponential growth attracts legal, ethical and operational challenges. The application of responsible AI and accountability has been dealt with by way of governments and organisations generating principles and guidelines for the creation and use of AI. This is a growing problem and falls short of an actionable solution. Accountability in the creation and use of AI is not and cannot be viewed as an extension of accountability as we know it. The dilution of responsibility is further complicated by not having independent audits, adherence to established standards, and enhanced compliance written into law, (Xia, Lu, Zhu, Lee, Liu and Xing, 2024)[13].

1.Emerging AI Remote Worker Technology

What defines AI lone worker technology as a product or service? AI lone worker technology can be described as the provision of a digital solution that provides real-time monitoring, regular communication with check-ins, and where necessary, rapid response for the well-being of the user. Which ensures a safer working environment. AI Technology has had a profound impact on the way we work. Over the past couple of decades, as the rate of technological evolution has picked up, the workplace has changed completely. But technology in the workplace is no longer limited to generating efficiency gains and maximizing profitability. It's also helping make workplaces safer. Because of rapid advancements in different fields, including data analytics, telecommunications, and safety monitoring, organisations can create a safe and secure work environment for their employees through emerging technology such as AI., (Bogdanović *et al,* 2022)[9]

But because of advancements in AI technology, it is difficult to comprehend or predict the future implications of the use of AI technology in remote worker surveillance in the home. There are threats as well as opportunities to our reliance on AI technology. AI has been the subject of debate at the European parliament level. They have enacted their first piece of legislation specific to the use of AI (European Parliament, 2023)[34] and (Clover, 2024)[18]. However, this legislation does not protect the rights of a worker to privacy in the home when AI monitoring technology is used. Rather, it merely gives weight to protection of a consumer or the general public when aligned with current GDPR laws.

This research will investigate whether the benefits of advancements in remote worker tracking technology outweigh the negatives. There are many aspects to the use of AI lone worker tracking technology that must be addressed on a continuous basis through various platforms to ensure the ethical use of this growing technology. One of the aims of this research is to demonstrate that although employee monitoring has existed for many years, advancing technology has changed the landscape for ever. Conventional monitoring pre-AI vs AI driven remote surveillance is that technological surveillance of employees intrudes into their private spaces.

For remote workers, audio and video surveillance may capture private spaces and conversations, raising the level of intrusiveness, (Centre for International Governance Innovation, 2021)[20]. The issue of artificial intelligence surveillant and monitoring employees

without regulation or safeguards is a concern. (Aloisi and Gramano, 2019)[1]. However, most interested parties may not yet know what their concerns should be or what safeguards to worker rights may be required when dealing with AI technology for the greater good of worker safety and relations. AI researchers who have identified potential ethical issues are themselves being sidelined and their views ignored, (Grodzinsky, Wolf and Miller, 2024)[42]. Current GDPR legislation and privacy by design were a measure of security against data breaches, (Romanou, 2018)[87]. This approach for data protection with regard to emerging AI technology is no longer suitable for the purposes as intended.

The pace of technology has outstripped relevance of safeguards implemented pre-2018. Since 2018, the pandemic could certainly be blamed for a lack in legislative progress in technology related privacy safeguards. But post pandemic and with the emergence of a greater number of home office workers, the need to revisit legislative powers is past due. Research suggests there is a lack of political will and a lack of understanding of IoT and AI capability to embrace the required changes. Many legislators are considering amendments to existing privacy laws. But, by the time legislation is enacted, it will be obsolete and not fit for purpose. The response of global power houses at an EU summit of the G7 was to advocate a voluntary code of conduct for AI development, (digital-strategy.ec.europa.eu, 2023)[26]. Global attitudes to governance are so unilateral in thinking. Although a single regulatory platform may not be practical, there may be little cohesive progress, (Cloete, 2024)[17].

2. Ethical use of remote tracking and surveillance information

This thesis explores the significance of transparency as an ethical imperative in tracking practices and its implications for lone worker tracking systems. Beyond the obvious safety benefits of using lone worker tracking. There could be valid concerns by employees or end users regarding the big brother aspect of tracking. Therefore. it is important to have clear guidelines and policies in place where remote tracking technology is used and where AI tracking is used. AI tracking technology has been identified as a rapidly advancing technology and therefore transparency in its use and capabilities is critical.

Accountability by employers plays a vital role as an ethical imperative in tracking practices, especially in the context of AI lone worker tracking. It entails open and clear communication

about the purpose, scope, and consequences of tracking activities. Transparency is essential in lone worker tracking to foster trust, respect privacy rights, and ensure informed decision-making. By providing comprehensive and accessible information about the tracking technologies in use, organizations demonstrate respect for the autonomy and privacy of lone workers.

Transparency allows workers to understand the data collected, the purpose for which it is used, who has access to it, and the potential impact on their well-being. The impact and suspicions of how or why data is used contributes to a worker's sense of vulnerability and is rooted in the approach to the ethical administration of monitoring, (Thiel, MacDougall and Bagdasarov, 2019)[102]. The promise of differential privacy does not yet appear to be addressed in employment law or indeed employee privacy legislation, specifically in relation to working from home. Differential privacy is a definition, not an algorithm, (Dwork and Roth, 2014)[29].

Current research does not appear to be extensive in demonstrating possible privacy issues for a remote employee. Employers and or their third-party tracking contractors harvesting employee data, do not differentiate between relevant and unacceptable data collection. Data linkage to nearby devices or technology has the potential to impact the worker and personal space and that of nearby occupants of the home. The potential threat of employers or third parties using private information is very real. Generally, linkage is becoming more pervasive as smart loT systems try to provide greater integrated coverage, (Zheng, Cai and Li, 2018)[115].

Building trust between employers and employees is essential when tracking technology is in use. Ultimately protection of data may be placed beyond the control of the remote worker and indeed an employer due to the exponential growth in IoT, AI and machine learning capabilities. When organizations are open about their tracking policies and procedures, workers are more likely to feel valued and respected. Honesty and communication empower workers to make informed decisions about their participation in tracking programs. This includes obtaining their consent based on a clear understanding of the benefits, risks, and rights associated with remote lone worker tracking. By seeking informed consent, organizations acknowledge the autonomy and dignity of workers, treating them as active participants rather than mere subjects of surveillance.

Ethical implications arise from the use of AI algorithms in tracking decisions, as biases and discriminatory outcomes can undermine fairness and non-discrimination. Organizations implementing AI lone worker tracking systems should actively address potential biases,

promote data diversity and representation, strive for algorithmic transparency, and establish mechanisms for accountability. By prioritizing fairness and non-discrimination, organizations can ensure that AI algorithms in tracking decisions uphold ethical standards and contribute to the safety and well-being of all lone workers, irrespective of personal characteristics. There are outstanding legal and ethical questions about employees' right to privacy. While monitoring employees is not a new phenomenon, how the data gathered is used is crucial. It is not sufficient to state surveillance is operating. An organisation must be very clear on the purpose of the monitoring and avoid extraneous use beyond that stated.

The capabilities and exponential growth in technology does require greater oversight. The advancement of AI for the purposes of surveillance does warrant updated legislation to protect employees, (www.legal-island.ie, n.d.)[63]. The European Union (EU) will consider a proposal to regulate artificial intelligence (AI) systems by adding to legacy data regulation acts. The intention is to create a framework to address evolving technologies such as AI. However, The USA as a leader in AI technology has yet to implement legislation on AI. This can only serve to hinder global cooperation between the USA and Europe, (Hillman, 2023)[48]. The fact that there is still a reluctance to implement robust legislation could expose those working from home to both unnecessary and potentially dangerous privacy invasion. The scope to misuse or create dual purpose technology for purposes other than stated or intended is a potential threat to an employee working from home and the general population, (Kritikos and Iphofen, 2023)[61].

If there is an "always on" technology within a private home, the potential to passively collect data is very real. Without the protection of legal frameworks to guard against such activities, society is vulnerable to abuse from the use of machine learning algorithms and advanced technology. There are growing concerns that AI Developers and AI owners should have been paying more attention to computing ethics. It is concerning when prominent AI researchers Gebru, Mitchell and Hinton at Google resign due to ethical concerns on the use and development of AI. For there to be an awareness by researchers at the heart of AI development for regulation and governance other than a motive for profit margins, is alarming, (Grodzinsky, Wolf and Miller, 2024)[42]. Yet, successive governments and legislators post Covid have demonstrated a lukewarm response to the debate and enactment of appropriate legislation.

While ongoing advancements in AI is exciting, the ethical implications on progression in AI should go beyond the theoretical aspect of AI. The danger to security and privacy is very real given we infuse AI intelligence into machines, interconnect gadgets, and in public and private

space, (V. Dankan Gowda et al., 2024)[107]. There is a need to be vigilant and cognisant of the invasive nature of an AI driven environment. While it should be a concern for society in general. The pervasive use of AI and IoT driven technology to monitor working from home has an impact on personal liberty and privacy. Where an employee works from home, they have limited recourse to identify an ethical use of data gathered. In terms of a work from home environment, a worker has little input into what may or may not be collected by any monitoring software in use. This has a direct impact on an expectation of privacy for the worker, family and occupants of the home. In the absence of legislation, a worker is at the mercy of the moral compass of an employer or robust employee supports such as Union membership or the power of numbers with a vested interest.

Advancements in AI technology and associated guidelines have little emphasis on ethics and fairness, (Kumar et al., 2023)[55]. This seems to be a global trend. Recent legislation proposed and due to be enacted has a light touch approach to what is currently at play with digital technology. The legislation is due to come into force in December 2024. However, AI owners, developers and users will have a further three years to put their house in order, (Mason Hayes Curran, 2024)[69]. In an environment where we are already playing catch on the potential pervasive nature of AI, does such legislation solve the gap in ethics and governance? This pending legislation certainly opens the channels of communication for a more robust framework and goes some way towards oversight. However, there is still not a global approach to AI governance and compliance. It is accepted that a "one size fits all" approach is not practical. But different legislation, at different levels, in different locations when there is global reach by AI technology, doesn't address the real weaknesses for compliance and governance.

3. Employees

The relationship between remote tracking and worker productivity has been the subject of numerous research including post-Covid, (Awada *et al,* 2021)[5] and (Torres and Orhan, 2023)[104]. By providing real-time insights into work patterns and highlighting potential areas for improvement, some research contends that specific monitoring metrics positively influence productivity. However, other research shows that excessive tracking might have a negative impact, increasing stress and decreasing creativity in workers. Job satisfaction and employee happiness are important aspects of how well an organisation performs. There is evidence of the

use of algorithms for surveillance causing discontent and resistance, (Kellogg, Valentine and Christin, 2020)[57]. According to the literature, excessive remote monitoring can cause emotions of mistrust and decreased job satisfaction, which in turn has an impact on staff retention and general organisational morale.

Research of workers pre Covid and within the employer's premises, has proven to attract negative opinions, 'I Don't Want Someone to Watch Me While I'm Working'. Workers felt vulnerable to surveillance, with women expressing more negative views, (Stark, Stanhaus and Anthony, 2020)[97]. It would be reasonable to conclude that attitudes to surveillance in the working from home environment would attract a greater sense of vulnerability. Research suggests that the negative impact of employee monitoring outweighs any positives as performance does not increase (Siegel, König and Lazar, 2022)[93].

Safety in the workplace is paramount for the well-being of an individual, colleagues, employers, and ultimately job security. Employees have a responsibility to ensure they adopt safety measures provided by their employer. However, does this responsibility extend to fully embracing remote lone worker technology? There is potential for an employee to feel aggrieved using tracking technology. The use of Biometric Tracking attracts a level of mistrust and disquiet even onsite, (Carpenter et al., 2016)[15]. Because of the rapid advancements and capabilities of technology such as AI. This has the potential to be viewed as an invasion of personal space and privacy.

The responsibilities of an employer to his worker are enshrined in law, (Electronic Irish Statute Book (eISB), 2005)[10]. While this regulation under several sections covers general health and safety obligations for the well-being of an employee. The development and use of the latest AI lone worker technology was most likely not envisaged at the time of enactment. It is also fair to say that aspects of health and safety are not considered in depth for the worker from home in terms of occupational health, (Montreuil and Lippel, 2003)[71]. While the principle of worker safety is legislated for, the use of AI as a means of worker safety leaves a variety of issues for the employer in terms of ethical behaviour towards an employee. Legislation relating to vehicle tracking by employers is in force, (Employer Vehicle Tracking | Data Protection Commission, n.d.)[32]. But this does not address the use of AI lone worker technology beyond an expectation of privacy under the European Convention of Human Rights. There is potential

for abuse of data collection like that of Barbulescu v Romania, (ECHR, 2020)[30] and (eela.eelc-updates.com, n.d.)[31].

The adaptability and speed of advancement of AI lone-worker technology has yet to be addressed in terms of data collection, retention, and use of such information by an employer for matters other than worker safety. Inclusion of employee viewpoints is important, (Alsos and Trygstad, 2023)[3]. The use of tracking surveillance technology in general could be concerning when used for worker analytics rather than safety, (Olsen, 2019)[77] and (Bernhardt, Kresge and Suleiman, 2023)[8]. Similarly does the use of surveillance tracking under the parameters of cyber safety serve to monitor possible cyberslacking by remote workers, (Luna *et al,* 2022)[65]. The use of employee monitoring in the workplace has attracted much debate on the fairness and appropriateness of doing so. In fact, there is a presumption on some level by an employee of a right to a certain amount of privacy in the workplace. However, according to a clarification by The Court of Human Rights on Article 8 states, the right to a private life at work, does not depend on an employee's reasonable expectations of privacy, (Atkinson, 2018)[4]. Legislation specifically in relation to protecting the privacy of those working from home does not appear to exist.

Based on research available and judicial challenges, the burden of protection seems to apply only when challenged. As a society we live in an extreme data driven surveillance realm. Research concludes that our every whim or desire can be tracked and monetised through various consumer driven platforms. The latest "data goldrush" has serious implications for an employee. It is well documented that consumer movements are tracked within the consumer world. There is the "always on" in terms of data collection. But, when that data extraction is performed in the workplace, which is the home environment for the remote worker. It impacts on a worker's privacy and freedom. In a situation where an employer has complete access to an employee's digital movements, it could potentially give the employer an advantage over the employee. Datafication of the worker while on and off the clock could adversely affect job security, promotion opportunities as well as bias and discrimination, (The Century Foundation, 2018)[101].

The additional stress of the use of new or advanced technology is concerning to employees. 40% of employees surveyed reported the use of new surveillance technology. It was also reported that there was a negative effect on employees in particular women. Compounding the

anxiety towards in the home surveillance was the fact employees were unsure of the type or level of surveillance. This suggests a lack of transparency or effective communication on the part of the employer, (Vitak and Zimmer, 2023)[99]. The use of AI to manage and supervise employees has proven to have an element of unfairness and bias. This can be problematic when a considerable number of managers rely on and trust the AI feedback, (Robert et al., 2020)[86].

When employees work remotely. There is greater potential for unfairness and bias. AI also presents new challenges to employees who are now both directed and held accountable by AI, (Hughes et al., 2019)[50]**.** Despite AI having many positive effects on an employee. There are also negatives in the form of insecurity and psychological stress. This can lead to employees feeling threatened in terms of job security. Effective communication and transparency could have a positive influence on an employee's perceptions of AI, where AI is integrated in employee performance and management, (Presbitero and Teng-Calleja, 2022)[82]. An employee's attitude towards AI within a work environment adopts greater importance when the worker is working from home. Where digital monitoring extends to the home, there can be a heightened sense of vulnerability.

4. Respecting Privacy Rights

Respecting privacy rights of an employee has entered a completely new phase for organisations. No longer is it the case that employee surveillance is within the actual domain of the employer. Although employees enjoy certain rights pertaining to an expectation of their privacy while actually onsite, should there be a breach of privacy rights, there is comfort in the fact that the issue is contained within the organisations working environs. When the home environment becomes the work environment, the right to privacy becomes paramount. There is still the power imbalance at play between an employer and employee.

There is use of more and more advanced technology since Covid 19, which have become more pervasive due to digital technology such as AI. This is concerning due to the indiscriminate collection of all manner of data, which may have little relevance to the employee as a worker,

(Vitak and Zimmer, 2023)[108]. The ability of emerging AI technology to understand and synthesise data collected rather than reproduce the data is concerning. The technology has the potential to collect any and all manner of data unsupervised, (Pieroni,2024)[80]. There is no specific legislation in the pipeline globally to address a threat to worker privacy, (European Commission, Joint Research Centre, Ball, 2021)[33]. There is little evidence of a meaningful discussion on this matter. There is an urgent need to engage with all stakeholders to establish a framework on worker rights and legislation to solidify an ethical charter and governance framework, (Kritikos, 2023)[59] and (Kritikos and Iphofen, 2023)[60].

Avoiding infringement of privacy rights requires a buy-in from all stakeholders, (Thiel, MacDougall and Bagdasarov,2019)[102]. Transparency is crucial in protecting the privacy rights of lone workers where organisations use remote lone worker tracking technology under the banner of employee safety and security. By openly communicating the extent and limitations of the proposed tracking activities, organisations demonstrate their commitment to safeguarding personal information, (Zanker *et al,* 2021)[114]. Transparency allows workers to understand how or why their data is collected, stored, or used. (Solove,2023)[96] Thereby fostering a sense of control over their personal information. Clear policies on data retention and access as well as mechanisms for reporting and addressing concerns are essential components of transparency in tracking practices. It also serves to promote the respect and value of an employee. Notably, unions are embracing the opportunities offered by AI technology for improvements in the workplace. However, this does come with valid reservations surrounding legislation where invisible technology is in use, (The Irish Congress of Trade Unions n.d.)[66].

Personal tracking which has evolved from asset tracking and can impact an employee. Privacy by design may be a tool to reduce the privacy impact on the end user (Jandl *et al,* 2021).[51] Workers during Covid remote working experienced excessive remote monitoring at times. Is this an abuse of privilege, (Hern, 2020)[45] The impact of Covid 19 thrust the employer/employee relationship into completely fresh territory. Adapting to a different type of performance management in terms of remote working post Covid may need to be redefined in terms of workforce strategies, (Göndöcs and Dörfler, 2021)[41]. Legislation in certain jurisdictions lags behind the pace of technology and in some instances is hampered by stakeholders' views on

complex issues surrounding privacy. A recent proposed US bill, The Workplace Technology Accountability Bill or AB1651 on workplace surveillance was deferred for that reason, (Kalish, 2022)[54].

It is inevitable that where legislation does not keep pace with technological advances, there will be a void between government oversight and that of a worker right to privacy. Nisenbaum's theory of contextual privacy does provide a framework to examine data collection and how it may violate privacy, (Nissenbaum, 2009)[75]. Contextual integrity is at risk when employees are invasively monitored and warrants closer examination, both morally and politically. There is however little evidence of political will in the form of legislation to address any potential violation of privacy. As identified in this research, the pace and intelligence of the latest technology may outstrip the pace of any future legislation, if it is based on existing information. The normalisation of employee surveillance within the onsite workplace does have consequences for employee wellbeing, work culture and motivation. Broader debates around information use, rights, power, and social structure highlights how surveillance in the workplace may serve to perpetuate existing inequalities and create new ones, (Ball, 2010)[6]**.** When that workplace is more often than not, the home, a more critical debate on surveillance and the technology used is even more relevant.

The emergence of fully-fledged AI systems in societies across the world is unlike anything experienced heretofore. The speed, scope, potential applications, and impact of AI after only a few months, has already been extremely disruptive. Are we exiting the 4th industrial revolution and being launched into a more sophisticated AI driven digital era. AI advancements necessitate appropriate governmental regulation, management, and oversight measures to ensure that its negative impacts are minimised, (Cloete, 2024)[17]. The difficulty for governments and legislators is one of supporting innovation and yet attempting to keep pace with the speed of progress in the digital area. Secondly, what should be regulated, given there is limited ability to adopt a "one size fits all" approach. Also, when dealing with AI in isolation. The known knowns and the potential for an unquantifiable level of unknowns, which could range from beneficial to harmful creates an uncertainty in terms of a roadmap for compliance or regulation, (Wheeler, 2023)[110]. Governance remains a challenge because different countries have competing priorities and strategies, (Dawson, Denford and Desouza, 2023)[23].

In terms of respecting a worker's right to privacy, the incentive to regulate AI in general falls short of what is required, (Dentons.com, 2023)[27]. It may be some time before legislation tailored towards regulating employee monitoring will emerge. Attitudes and beliefs towards information privacy today are not dissimilar to those researched in the pre digital age, (Stone et al., 1983)[98]. Workers from home, who now live in an age of constant information monitoring and dissemination could arguably experience additional fears relating to privacy. Zuboff has coined the phrase "Surveillance capitalism". There is evidence of extreme concentrations of knowledge generated, free from oversight. The threat to 21st century society because of a digital cross connection is identified by Zuboff as a powerful tool to predict and or control our behaviour, (Zuboff, 2023)[116]. This research implies a threat to the privacy of a worker while working from home.

There is usually an expectation of privacy or at least an expectation of choice to opt in or out of data collection. But, due to the interconnectivity of digital devices, the "always on" status comes into play. Given, the worker is remote, indiscriminate data collection may be taking place. The potential harm to an employee due to the direct manipulation and leveraging of information harvested is quite possible in terms of bias, salary negotiation or promotions. There is also the impact of the use of passively collected data for the purposes of third-party gain. Whether the data is harvested by design or unintentional. The net effect for the working from home employee is a disregard for the respect and expectation of privacy as a right. The ability of IoT and AI to cross reference and synthesise information within an environment is concerning. While a single digital interaction may offer anonymity. The collection and convergence of data has the potential to identify a person and sensitive information of the person being monitored.

5. Informed Decision Making

Transparency promotes informed decision-making for an employee. Organisations must communicate the goals, benefits, and limitations of AI lone worker technology. Allowing workers to assess the potential trade-offs between safety and privacy. Transparency empowers workers to evaluate the risks and benefits or to voice any concerns they may have. Informed

decision making ensures the workers understand the implications of being tracked and provides an opportunity for their input on design and implementation of an AI powered tracking system, (Schoenherr *et al,* 2023)[92]. Transparency serves as an ethical imperative in tracking practices particularly in the context of AI lone worker tracking systems. Openness fosters trust enables informed decision making and protects privacy rights,

Organisations considering or implementing AI lone worker tracking systems should prioritise transparency by providing clear and accessible information to their workers, seeking informed consent, respecting privacy rights, and promoting open dialogue. By embracing transparency, companies can navigate the ethical complexities of AI lone worker tracking and foster a culture of trust and respect in the workplace. The promotion of human-centric AI technology should be a priority for decision makers in the workplace. (Krzywdzinski, Gerst and Butollo,2022)[62]. Psychological concerns towards privacy and tracking data can result in negative attitudes, (Ketelaar and van Balen, 2018)[58].

The influence of AI Algorithms in tracking decisions in the context of lone worker tracking could be open to discrimination and bias.AI Algorithms are designed to process large amounts of data and make predictions or decisions based on patterns and correlations. In the context of lone worker tracking, AI algorithms analyse a variety of inputs, such as location data, biometric information, and environmental conditions to assess a worker's safety and to trigger alerts or allow interventions. However, the algorithms can inadvertently introduce biases or result in discriminatory outcomes and behaviour due to the data they are trained on and the inherent limitations of algorithmic decision making, (McKendrick and Thurai, 2022)[70].

Acceptance of the use of employee monitoring on the part of the employee should be on the basis of making an informed choice and accepting the trade-off of benefits and reward against actual privacy risk or a perceived risk. In addition, smart technology has the ability to gather large amounts of personal information automatically without the employee being an active participant or knowing its intended purpose, (Princi and Krämer, 2019)[84]. There is a need for a very specific range of managerial competencies with the increased use of AI within the working environment. It is not sufficient or acceptable to plead ignorance. This can ultimately lead to mistrust within the work place. Where the work place is in fact the home, this becomes even more important. The integration of artificial intelligence (AI) mandates a paradigm shift in

managerial and organisational competencies. The ability to scrutinise AI systems for biases, champion fairness, and navigate the ethical intricacies of AI decision making is paramount, (Moore, 2024)[72].

The development of computers and calculators have gone through many phases of development and understanding. The appearance of analogue and digital computers from the turn of the 20th Century served as a platform for future advancements. By the time fifth generation computers were developed, this was proclaimed the super computer of the future. However, all computing on a theoretical level focus on the application of Boolean logic, even AI. The study of informatics is a relatively new subject. It studies data searching and collection, storage of data, and the conversion and use of information in different areas of human activity, (Tsvetkov,2023)[105] . The study of informatics has gone through many phases researching from first to fifth generation computing on a theoretical and engineering scientific basis. It does not however consider the implications of computer-generated AI in the context of human interaction or a right to privacy.

In terms of informed decision making, theoretically an AI driven application can and will collect data indiscriminately. The ability to understand and synthesise the data collected is considerable. Advancements are hailed as progress; however, ethical weaknesses do not appear to be addressed by products owners. When no regulatory framework exists, or defined legislation enacted. The desire to improve may be absent unless incentivised by potential profit or society. Self-regulation is not the way forward for such a crucial innovation with far reaching consequences for humanity. It is incumbent upon employers to become AI literate, rather than just be aware in the context of information delivery to employees. AI literacy is an important enabler for informed decision making in the data age, (Schneider and Weber, 2024)[95]. However, there is the potential for AI models' behaviours to be skewed. Because AI systems are created by humans, the introduction of biases whether deliberate of incidental, raises concerns about informed decision making and free will. Does the choices made by a developer including ethical considerations impact an outcome, (Danaher, 2020)[22]. Even where a developer or AI system operates with the best of intentions. The potential for abuse of information is very real given IoT engage in extraction of information across connected

devices. Coupled with AI, the need for human intervention in decision making is either entirely irrelevant or minimal.

The research therefore questions whether we can truly make an informed decision on the use of IoT and AI generated technology in the work from home environment. For the remote worker, does a worker need to disconnect all devices apart from a work-related device to avoid cross contamination of information. There is also a suspicion that algorithmic nudging can alter a decision. As a positive, advances in AI personalized nudges have the potential to improve our lives. As a negative, where black box nudging is blindly outsourced, the unknown cognitive process they harness may go unchecked. Given we are still in a state of little oversight beyond self-regulation, this is potentially an undesirable position to be in. It strikes at the very heart of informed decision making when you don't know for sure what processes are in play, (Schmauder et al., 2023)[94].

Literature Conclusion

It is clear from the research that an approach to ensuring workers right to privacy while working from home may not be delivered by a "one size fits all" approach. Globally legislators are lagging behind on a clear direction to deal with infringement on a worker's right to privacy.

The Covid 19 pandemic disruption to industry and services was unprecedented and a considerable number of organisations adopted the use of remote working rather hurriedly to satisfy operational needs. At the time, both employers and employees embraced the situation to keep as many areas as possible operational during the lockdown. For an employee this was important for an income and to preserve their employment status. Ultimately the co-operation of the work force, albeit in the main for self-preservation, assisted organisations to maintain services and revenue streams in a difficult environment.

The advent of remote working as a mainstream choice was born. Prior to the pandemic most organisations with a few exceptions were firmly based onsite. Those who worked remotely, prior to lockdown was by choice or accepted as part of the Gig economy. More often than not,

the trade-off between flexibility and a job was the deciding factor on working remotely. However, the emergence of AI technology and the advancements of IoT is a transformative power within our working world. During the pandemic and post pandemic, remote technology assistance demonstrates that a considerable number of occupations can be done remotely.

The research suggests that advancements in such technology could arguably be viewed as a double-edged sword. The intelligence of AI and the use of algorithms and machine learning are undoubtedly a positive aspect of progress. However, with the speed of developing technology, comes great responsibility for legislators. Governance, ethics, respect for privacy rights, informed decision making all appear to have taken on a role of lesser importance in the name of progress. There are certainly advancements and awareness in terms of wellness and mental health. It is notable that most legislation post pandemic regarding remote working focusses on the right to work remotely as an employment right and the effects of working remotely on the wellbeing or safety of an employee. The drive to protect basic worker rights through legislation is admirable. Yet, one of the most fundamental rights to that of a worker's right to privacy while working remotely has not been legislated upon post pandemic. Legislation on a worker's privacy right while at work pre pandemic were at best borderline sufficient to protect a worker and triggered several court cases on various abuses through the use of monitoring surveillance for purposes other than safety or tracking work progress.

Based on the lack of new legislation or debate within political institutions or the political will to move towards correcting this anomaly. There is a very real danger to individual privacy and a potential risk to information security at a national and global level. The impact of the 4th industrial revolution will have far reaching consequences on ethics, privacy, and governance globally. The world seems ill prepared to navigate the consequences of not addressing the challenges of AI and IoT through a robust framework or road map. Ignoring the fundamental right to privacy of a remote worker may be a catalyst to a greater oversight issue in terms of cybersecurity and the management of technology.

The research provided, demonstrates a paucity in meaningful safeguards to protect the privacy rights of workers either while on site, or most importantly within the home environs. Unfortunately, in the absence of governance of AI and other technologies in the digital era, the

use of employee surveillance is open to abuse. The purpose of this research is to highlight the lack of oversight and governance during the progression of the digital era.

Research Methodology

The research question asks: Does employee monitoring impact on workers' right to privacy, while working from home?

Research Model

The research was qualitative in approach and nature, as it is a method that seeks to examine and reflect on perceptions. And to gain an understanding of how a respondents feel about a particular topic, (Collis and Hussey, 2014)[21]

Aim of the research

This research study was undertaken to contribute to closing the gap in the existing literature with regard to the impact on privacy of an employee. The use of employee monitoring technology while working from home was investigated. The survey asked the respondents a number of questions related to their experience of being monitored as an employee. Specific questions were asked of each respondent regarding their knowledge and opinions on being monitored as a remote worker. The questions were asked in order to satisfy a number of objectives that the researcher set for the study. This section will provide the reader with an overview of the results.

Is there a case to be answered regarding the monitoring of employees, in particular in a remote setting, such as the home environment? It is important to establish if there is an impact on employees right to privacy due to the exponential growth in AI technology and the digital era.

Most research papers to date have investigated the overall impact on an employee working from home in terms of wellbeing, burnout and the "always on" pressure.

Invasion of privacy has not been researched in great detail as a standalone issue for those working from home. However, most research has flagged the undeniable capabilities of the digital era. This research investigates issues surrounding the use of technology to monitor employees in their homes. The research seeks to identify a solution to the research question asked. The survey participants provide an insight into how monitoring technology is viewed by them as employees. Respondents were consistent in their views on privacy and fears.

Previous research on attitudes to privacy concur with modern day opinion on the perceived level of control over their private information and satisfaction with actual control, (Stone et al., 1983)[98]. Respondents appear to be ill equipped to deal with remote monitoring technology, choice does not seem to be an option, as they have never been asked by an employer if they agree to be monitored. However, some respondents are of the view that it is embedded somewhere, deep within their terms and conditions of their employment contracts. The trade-off is either working from home as a choice or a condition of employment. Ultimately, regulation on the practice of employee monitoring in the home lies with legislation, governance, and a global framework beyond borders, to address the invasiveness of surveillance technology. A global framework is important as a considerable number of employees work for international organisations and their headquarters may or may not be in the jurisdiction of an employee.

Key concerns would be, what type of data is collected and stored? How will the data be used by an employer or their agents? What protections are in place to protect an employee and those in proximity to the employee against invasive monitoring technology? In the event of a cyber-attack, how is the employee protected from harm?

1. Research Collection Methodology

The researcher reviewed and interpreted information collated with an emphasis on the impact of employee monitoring on privacy within the home. Although the outcome is interpretive, the problem was identified and evaluated using a systematic approach to quality data harvested from survey data. According to best practice, the research was systematic, and the data was

carefully collected, analysed and considered to arrive at the research conclusion, Qualitative research is defined in terms of the trustworthiness of the data and findings, (Nassaji, 2020)[75].

The research paper is using qualitative methods for the purposes of research findings. Qualitative research is based on methods of observation and inquiry; qualitative research "explores the meaning of human experiences and creates the possibilities of change through raised awareness and purposeful action, (Taylor & Francis, 2013)[100]. Data analysis is central to credible qualitative research. The researcher, through analysis displays an ability to understand, and interpret findings. Which is crucial to uncovering meaning in particular circumstances and contexts, (Braun and Clarke, 2022)[11].

The purpose of the research is exploratory. The thematic analysis evolved from the content analysis, (Braun and Clarke, 2016)[12]. The research method used is appropriate to the research question. A survey of 26 participants was undertaken to support the analysis of the research question. (Creswell & Creswell, 2018). The use of 26 participants was deemed appropriate for the research question and assisted by considering the findings of Fugard and Potts on achieving a suitable sample size in terms of investigating patterns, (Fugard and Potts, 2014)[37].

The focus of the research will be assisted by the thematic analysis of the data harvested in addition to peer-reviewed journal research. A number of news articles and conference papers were also used to demonstrate the fluid nature of developing technology and to highlight the subject of AI progression discussed during conferences or government discussions on legislation. Thematic analysis is the process of identifying patterns or themes within qualitative data, (Braun and Clarke, 2022)[11]. The use of inductive logic and research will be focussed on the emergent nature of the research question. Emergent elements of qualitative research can be described as acceptance of adapting inquiry as understanding deepens and/or situations change. The researcher avoids rigid designs that eliminate responding to opportunities to pursue new paths of discovery as they emerge, (Lincoln and Denzin, 2009)[64]. Induction generally relies on accumulation of positive instances in order to verify a theory as correct. (Depoy, 2016)[25]. Technology in remote working monitoring has the potential to accelerate at an extraordinary pace, in particular with the emergence of AI assisted machine learning, (Ozatay et al., n.d.)[78]. Therefore, a broader focus on available data was applied due to the emergent aspect of information relative to the research question.

2.Data Collection and Sampling Criteria

Participants of the survey were not randomised. They will have experience of being the end user voluntarily or because of employment requirements. Respondents are employed in various categories of seniority within their respective organisations. Survey participants are from industries such as financial services, banking industry, utility services, education administration, technology providers, insurance services, pharmaceutical industry, and recruitment.

Study inclusion criteria were (a) at least 18 years old and in fulltime employment, (b) working remotely during and post Covid 19 pandemic, (c) working remotely pre Covid 19 was not excluded, (d) self-employed or contractor status were excluded.
There were no set requirements for the number of hours worked remotely or the hours the study participants worked. Seniority level was not considered.

The chosen interview method was via email following an introductory call or message. The interview data was collected entirely online via email using The Microsoft Forms Survey software. The survey tag line was Remote Working: Convenient or curse? A total of six questions were asked of each participant. Respondents were asked to avoid Yes/No/N/A answers. (Appendix 1) An information sheet outlining the purpose of the research survey was provided to all participants. A consent form was also generated prior to participating in the survey. (Appendix 2)

The data gathered was qualitative in nature. A decision to have an open-ended question style was because personal experiences and views can differ greatly on this subject. It was also interesting to collect data from respondents in a variety of industries. All data collected was anonymised. Data storage was on a local computer, an associated external hard drive and The National College of Ireland student OneDrive.

3.Survey Questions

Respondents were asked six open ended questions. They were requested where possible to avoid YES/NO/N/A answers. They also had the option to not answer a question.

1.How do you feel about employee monitoring while working remotely?

2.Do you think there is enough transparency surrounding the type of monitoring technology used, especially with advancements in technology?

3.Does it concern you that monitoring may impact your privacy?

4.Have you ever requested additional information on the type and purpose of monitoring software?

5.If you were concerned about the use of monitoring software or purpose, do you feel you could raise this with an Employer?

6.Would you be concerned that monitoring software may imply a lack of trust by an employer or a sense that your work ethic is in question? If you had a choice, would you agree to remote monitoring technology?

Link to survey result: https://bit.ly/4dMugrh [99]

4.Data Collection Method

The research included pretest of a single participant rather than a pilot study. This was to ensure the questionnaire was clearly articulated, was relevant to the purpose of the survey and allowed assessment of response latency, (Hashim et al., 2022)[43]. The use of a pilot study was excluded from consideration due to the small sample size intended for the main study. The pretest result was used as an an opportunity to refine the interview question and layout if required, (Presser et al., 2005)[83]. The pretest data collection and administration method were adopted throughout the survey. The pretest data has been included in the result. Total respondents were 26 including pretest. The data gathered was qualitative in nature and was measured by thematic analysis.

For this research, data was harvested for research information from several journal sites, government websites and European worker and human rights sites. Tracking industry product specifications were considered and investigated to mitigate and avoid research bias. The literature review formed a valuable part of the research process and assisted with the formation of the survey questions.

Research data was collected with methodological and ethical recommendations advocated by Saunders et al (Saunders, Lewis and Thornhill, 2019)[90] ,and (Saunders et al., 2019)[91] updated 8th Edition.

5.Research Limitations

The research data did not differentiate between remote working as a lifestyle choice, hybrid or an employment criterion. The relevance of an industry sector or job category was not considered in the overall research or data collection. The research did not investigate a link between gender, age or status in terms of views on employee monitoring or worker privacy rights. The research did not consider the social environment of the worker from home in terms of whether they were co habiting, family relationships or the availability of a dedicated home office space.

There is a danger that assumptions could be made that a worker holds a certain view on privacy rights because of personality rather than the actions of an employer within an industry sector or job category. The "Big Five" personality dimension agrees there is a distinct relationship between personality and job performance, (Barrick and Mount, 1991)[7]. This could detract from a very real modern-day issue whereby advancements in technology in particular AI have outstripped pace on legislation required for remote employee surveillance. The type of remote technology in use by organisations was not considered in terms of surveillance capabilities and possible impacts on a worker's privacy. Cybersecurity vulnerabilities were not investigated in detail beyond potential access to private employee information.

6.Future Research Scope

There is potential to further research within a specific industry sector or a specific job category or seniority level or indeed respondent age bracket. Research could seek to explore the relationship between employee monitoring views within a particular industry or specifically per job category. Research of the particular types of technology employed may also give weight to an employee's views on infringement of privacy rights. In the event that legislation is enacted, research on whether an employer or employee's views differ post legislation, may give greater insight into acceptance of the use of particular types of technology.

7.Survey Data Analysis

Themes Emerging from Survey Data

Themes identified during the data collection were consistent across all respondents. The results were not unlike views expressed in existing research literature, (Ketelaar and van Balen, 2018)[58] .

1. Lack of transparency
2. Privacy concerns
3. Disagreement with being monitored under any circumstances
4. Implied lack of trust

To be fair, there wasn't an outright distain for monitoring, (Figure 1). In some instances, Respondents found remote employee monitoring may be warranted and were accepting of it under certain circumstances such as lack of employee performance or project specific adherence to deadlines. Respondents did not agree with monitoring of performance, when all workloads or projects were submitted on time and of an expected quality. However, 10 participants felt that it was dependant on why the monitoring was required. The view was it should only be exercised strictly under the understanding of absolute transparency in all cases. 15 respondents disagreed with monitoring entirely as it made them uncomfortable, or it inferred a lack of trust. There was no evidence of active surveillance resistance by respondents similar to that in other research, (Kellogg, Valentine and Christin, 2020)[57]. However, it is difficult to conclude, is this because of an accepted trade-off between the ability to remote work versus onsite or an acceptance of advances in digital technology post Covid to allow remote working?

Transparency

Lack of transparency was interesting insofar as 18 stated there was a total lack of transparency or a minimal level of openness. This number is similar to that of those disagreeing (20) with monitoring entirely. Does lack of transparency contribute to an employee's view on being monitored, (Princi and Krämer, 2019)[84]. It would be reasonable to conclude a lack of transparency does influence a point of view. Only 3 respondents felt secure with the amount of knowledge they had from their employer regarding monitoring. However, all respondents bar one was unsure of the level of monitoring. Lack of information and transparency is viewed as important to workers, where monitoring post Covid has become normalised. Within the trade-

off on the convenience of working remotely, there is bargaining and consideration of where to draw the line on what is acceptable, (Vitak and Zimmer, 2023)[109]. The one respondent with knowledge of how they are being monitored, has the option to turn off monitoring and is in control of when they are monitored. Therefore, while one respondent can be satisfied that they are in control, the remaining respondents are experiencing a paucity of information of an unacceptable level. However, do we really know what is transparent when we include AI nudging, (Schmauder et al., 2023)[94]. An organisation most likely will buy an off the shelf platform, no respondent was able to say what is used in their workplace. Beyond the face value of the system working and generating the required data, an employer has no way of knowing what is on the back end of the software, unless they ask. This would require more than a cursory knowledge of AI driven digital technology. So, we have a situation where the employer may not have all the facts and a product owner who has no fear of sanctions within the current lack of oversight. Even if an employer were to draft an information sheet for employees. The type and purpose of data collection may be questionable beyond the stated purpose.

Most participants said they could ask their immediate superior or HR about the use of monitoring software. Although a large portion stated that asking would not make a difference in so far as monitoring would continue due to the size of the employer. Some felt they wouldn't know if monitoring was active due to lack of transparency. 3 felt they couldn't ask as it might be perceived as guilt or being difficult. The research suggests that many would not know what should be asked of an employer, even if they were to ask. However, there is an added consideration for employees to navigate where employees are now both directed and held accountable by AI. (Hughes et al., 2019)[50]. Effective communication and transparency with employees would make a positive impact, especially when respondents were suspicious of employee monitoring, (Presbitero and Teng-Calleja, 2022)[82].

Privacy Concerns

Privacy concerns were striking and 20 out of 26 respondents had reservations that monitoring is or may impact on their privacy. Again, transparency or lack of, is a major contributor to the viewpoint. Several respondents deliberately cover their cameras as they are unsure. But those with a technical background point out that their microphones may be the subject of monitoring also. The majority of respondents found monitoring to be invasive. 5 believed it was part of the job and had no expectation of privacy. For those who had no expectation of privacy, it is unclear

what their personal status or living arrangements are and this may contribute to their opinion on this. A concern for privacy may not be an unreasonable view, if linked back to research on surveillance capitalism, (Zuboff, 2023)[116].

Disagreement with being monitored under any circumstances

Most respondents do not agree with remote monitoring and if they had an absolute choice. They would reject all forms of monitoring, in particular in the home. As identified in the literature research, a considerable number of respondents feel, they are more than capable of completing tasks efficiently and on time without supervision, (Hern, 2020)[45]. There was an inherent sense of suspicion of covert monitoring taking place and a sense that their personal space was being monitored or there was the potential to do so. A considerable number surveyed (20 out of 26) have strong concerns that their privacy is already or may be impacted. This is compounded by being unsure of when or why they are being monitored. The use of, for instance biometric technology raises privacy concerns whether real or perceived. It instils a sense of mistrust towards an organisation, (Carpenter et al., 2016)[15]. Notably, respondents have never asked their employers if they are being actively monitored, the type of monitoring, what the data is being used for or if it is stored. Is there an argument to be made that employees don't feel secure about asking or making their views known, simply because they don't have the backing of legislation, (Aloisi and Gramano, 2019)[1]**.** As indicated in the literature review, many people may not have the knowledge or understanding of technology used in the digital era to ask the relevant question pertaining to an invasion of privacy. There are many aspects of privacy not considered by many, where the use of AI is involved, (Van Rijmenam, 2023)[104]. One respondent admitted they never considered an impact on privacy. However, 17 respondents did feel they could ask, with a further 4 of the view it would reflect badly on them if they asked. 5, although had no reservations about asking felt a query would be pointless as the conditions would not change should they query or object to monitoring.

Implied Lack of Trust

Most participants said they could ask their immediate superior or HR about the use of monitoring software. Although a large portion stated that asking would not make a difference in so far as monitoring would continue due to the size of the employer. Some felt they wouldn't know if monitoring was active due to lack of transparency. 3 felt they couldn't ask as it might be perceived as guilt or being difficult. The research suggests that many would not know what

should be asked of an employer, even if they were to ask. However, there is an added consideration for employees to navigate where employees are now both directed and held accountable by AI. (Hughes et al., 2019)[50]. Effective communication and transparency with employees would make a positive impact, especially when respondents were suspicious of employee monitoring, (Presbitero and Teng-Calleja, 2022)[82].

In some instances, the use of employee surveillance may be harmful to an organisation because of suspicion and lack of trust on all sides. Perception or reality impacts on the relationship between the workforce and employer, (Home of internet privacy, 2021)[49]. The concerns of the end user must not be taken lightly, (Morgan and Nolan, 2023)[73].

8.Research Methodology Discussion

Most researchers tend to design their research to answer a question or identify a problem. They begin by working out what data are needed and what method, tools or techniques should be used. This means that they start peeling the onion from the center, (Sahay, 2016)[88]. To address any short comings in choice of methods used , the researcher investigated all aspects of research through the study of the research onion, (Figure 2).

Due to the sample size, triangulation of data would not benefit the conclusion or validity of the qualitative data. Credibility is reliant on the industry experience of the researcher and the responses of the survey participants. The author was careful not to introduce bias in the findings. The research relied on the concept of thick description as a means to validate the data, (Ponterotto, 2015)[81].

Research philosophy refers to a system of beliefs and assumptions about the development of knowledge. Development of new knowledge regardless of the existence of existing knowledge, is still a development of new knowledge. Certain unconscious assumptions may be made during the research process, (Burrell and Morgan, 1983)[14]. According to Pallagola, researchers are guided by their perceptions and assumptions, rather than free will, (Palagolla, 2016)[79].

Ethical considerations

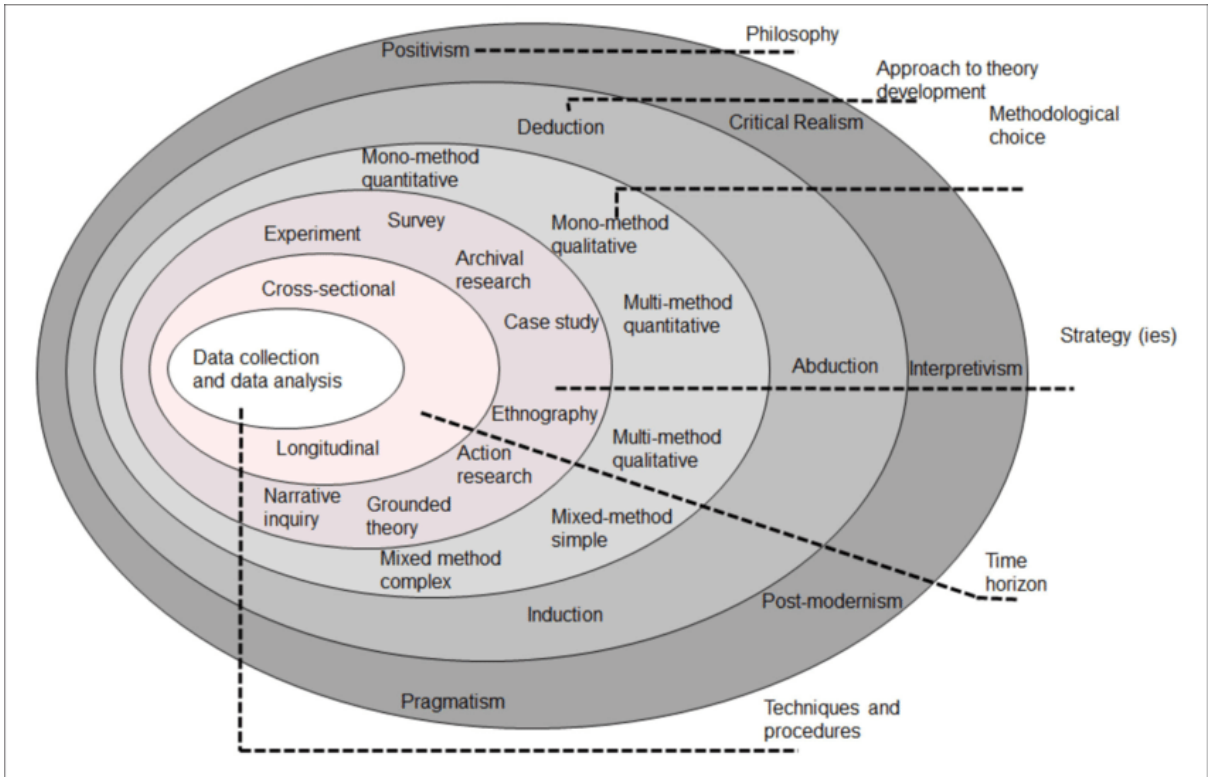
Regarding ethical considerations, (Saunders at al, 2016) state the importance of complying with the appropriate code of ethics. Respondents are anonymous, and 26 consent to use the data was handled by the questionnaire.

All subjects who were approached were contacted with complete transparency as to the purpose of the project and how their data would be used and stored. They were assured that confidentiality would be maintained through the process as would their anonymity. This was done via email with the survey invite. Permission to use the survey data was stated as implied, if the respondent returned the survey. However, they were also given the opportunity to rescind their permission up until the point that the data was submitted.

The Research Onion

The researcher used the Research Onion, (Saunders et. al 2019). The use of the Research Onion guided the researcher in making the appropriate decision on the methodology to use. The research onion is a tool that helps to direct research and develop a research design by systematically moving through each layer. Identifying the research methodology most useful for the research, follows a certain structure. It commences with outlining the fundamental philosophy, followed by the identification of methodology, and strategies. Based on in depth analysis of the Research Onion, a qualitative methodology was adopted for this study. Methodology refers to a comprehensive research approach that is appropriate to conduct of research. It forms a suite of principles and philosophical assumptions that shape the comprehension of the research inquiry and results. Research methodology is a vital component of a thesis. The use of techniques, and underpinning philosophy support the outcome. The Research Onion serves as a visual representation of all methodological approaches. It gives clarity to the most suitable technique for doing research and collecting data relative to the research question. The many layers of the Research Onion can provide and guide the selection method used. The research paper plan and design is an important starting point of the research methodology. The research method used must be capable of explaining and justifying the approach used. Therefore, due attention should be paid to philosophical assumptions underlying one's research, (Tjano,2023)[103]. Research categories can be divided into categories that influence how a researcher approaches their study: ontology, epistemology, and axiology (Saunders et al., 2015).

Figure 2



The purpose of the research was to investigate and validate if there was an impact on a worker's privacy while working from home. The use of thematic analysis was identified as the most appropriate research method. The methodology employed was assisted by research literature relevant to the question of employee monitoring. While there was limited research available

with specific focus on privacy rights of the remote worker. This paper narrowed the focus to aspects of employee monitoring that could reasonably be assumed would impact a worker's right to privacy while working from home.

By grouping responses, the researcher identified a common thread in all questions answered. The use of open-ended questions further validates that employee monitoring of a worker while working from home does have a negative impact on an employee's right to privacy. There was at a minimum a view by a considerable number of those surveyed that a privacy issue exists. Whether this is perceived, or a fact isn't entirely verifiable as the types of surveillant technology used was not identified by the respondents. It was also notable that of the 26 respondents, only one had total knowledge of the type of technology installed. Research methodology is the application of specific procedures to process and analyse information for the purposes of gaining insight into a subject matter. Notwithstanding the research limitations identified under methodology research limitations, section 6. The research question has demonstrated a distinct lack of clarity surrounding employee monitoring within the home office.

Employee monitoring has existed pre-technology in the form of in-person supervision, collection of proof of working time through a paper trail, or through assessment of actual work completed in the time allotted (Groen *et al.* 2018)[40].

Remote working throughout Covid 19 and the availability thereafter of remote or hybrid options have become more popular. Digital, IoT and AI technology has impacted how we approach working time supervision. The research is relevant to lone or remote worker tracking with the use of technology such as IoT and AI in the digital era. The research seeks to investigate the ethical aspect of using IoT and AI tracking technology for lone worker safety and supervision.

A particular focus of the research was on transparency, fairness, and inclusivity of the worker in decision-making. There is a less-than-ideal approach to ethics and a governance framework in how AI is developed. Theory and practice gaps exist in the management of AI ethics and application, (Sanderson et al., 2024)[89].

Overtly, the benefits and convenience of lone worker tracking technology presents an argument for use, given that such systems do enhance operations. But at what cost beyond the initial investment. Once one delves beyond the gloss of convenience, the question is whether the benefits outweigh the negatives.

Remote worker tracking technology offers the advantage of addressing safety obligations and monitoring services to the employer. Several commercial sites offer a variety of off-the-shelf AI-assisted tracking services. The question is, where is the data collected stored and what is the data used for. Could there be a danger of abuse of privilege? Similarly, remote worker tracking systems do provide a measure of security to the employee working in isolation with a positive impact on their personal safety. There must be criteria and structured mechanisms to deal with employee queries and doubts where lone worker tracking technology is not fully understood or embraced by the end user.

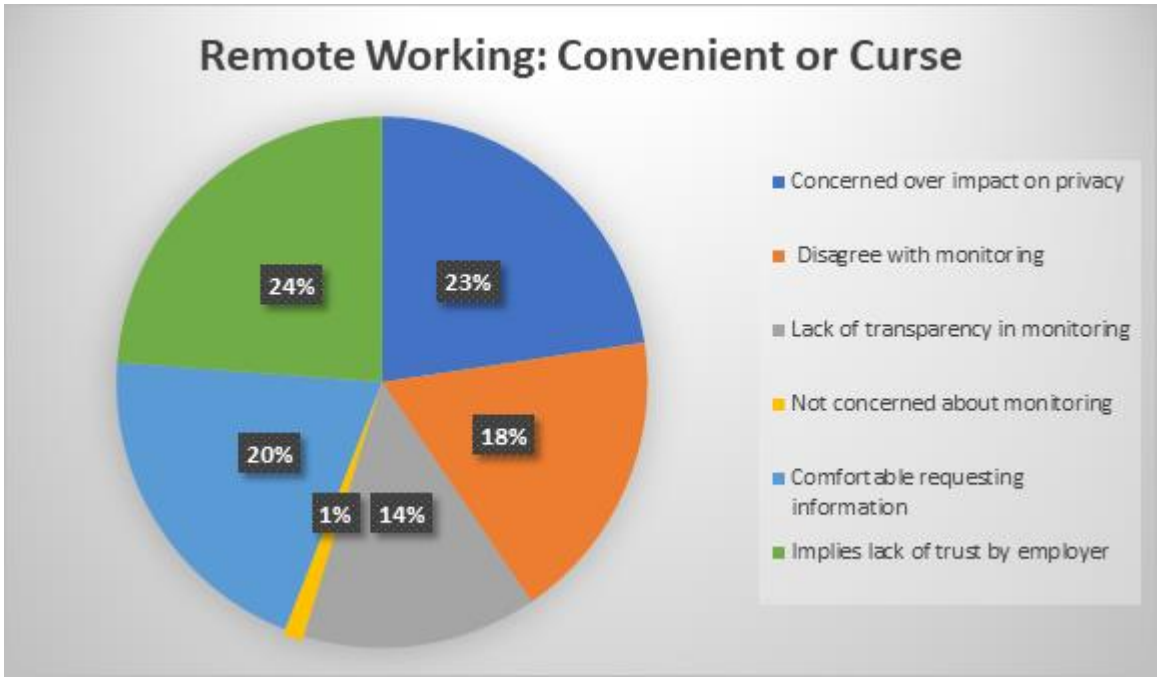
In order to extract a credible answer to the research question: Does employee monitoring infringe on workers' right to privacy while working from home? The answers to the six questions were coded into themes. There were specific themes which emerged through all questions on analysis of the data generated from the survey. These themes were as follows: a disagreement with remote monitoring as part of the job, concerns over privacy, either lack of or minimal transparency, implications surrounding trust and employee performance, and some respondents felt it was dependant on circumstances. However, the overall opinion from respondents is undeniable in so far as almost 80% of remote working employees has various concerns relating to employee monitoring regardless of the purpose. The researcher aimed to narrow the focus as much as practical to the subject of employee monitoring within the home. The influence of subject intentionality is very relevant to the research outcome, (Chesebro and Borisoff, 2007)[16].

Overall, when privacy concerns, lack of transparency, implied lack of trust, and disagreement with monitoring are considered collectively. There is an overwhelming sense of dissatisfaction with employee monitoring, by employees. Existing research regarding trust within an organisation does appear to align with the views of the survey participants data, (Carpenter et al., 2016)[15]. It was interesting that a number of respondents were unsure about transparency pertaining to monitoring and one respondent hadn't even considered an impact on privacy. Equally, it must be stated that a number of respondents considered that monitoring comes with the job, and in particular, if working remotely.

To assist visually with the survey results, a Pie Chart, (Figure 1) was created using the quantitative data answers as a percentage of each answer. The only aspects of the answers used

for the chart are as listed in the pie chart analysis descriptions. Please note, beyond a visual aid, the data captured was not analysed in depth quantitatively. The answers to the open-ended questions were collated to significant themes emerging in the surveys returned.

Figure 1



Thesis Conclusion

The overall conclusion based on the literature review and methodology, is there is a threat and impact to a worker's right to privacy on some level. There is a potential for data collected from a worker's home to be used for purposes beyond working time. Lack of transparency combined with a knowledge of what AI is capable of, contributes to employee views on surveillance in the home office. There is an uncertainty regarding what data is collected. In so far as, is it truly anonymised and what is the purpose of the data. Most people are accepting of the fact that when you step outside the home, data can and will be captured. Some aspects of the digital era are very clear in terms of the capabilities of IoT and AI technology. There is an acceptance that the use of technology in the digital era is here to stay. However, there is an expectation that once within the safety and security of the home, privacy should be under the control of the

inhabitant. Workers from home thus far must deal with the imbalance of power and the accepted trade off of diminished privacy while working from home. There is a sense from the respondents and the literature review that the protection of a worker within a home office setting is not a priority beyond basic health and safety. Worker privacy rights while onsite are also experiencing similar privacy issues as labour laws have not kept pace with the digital era. There is little incentive for an employer to address short comings or misgivings by an employee. The lack of a coherent and robust policy on the use of digital technology allows organisations to disregard an employee complaint regarding remote monitoring. Research suggests many employees would feel they couldn't raise the issue of monitoring or its purpose.

Few could have envisaged the explosion of AI and IoT development and capability to the extent it was at during and post Covid. The occurrence of Covid 19 which affected the whole world was unprecedented. The world didn't stop turning because of Covid and to be fair the scramble to keep the wheels of commerce turning was accomplished through a willingness by all to step up to the challenge. The opportunity to roll out the latest iterations in IoT and AI at speed presented itself in the form of mitigating disruption from various restrictions of movement and total lockdown. The use of surveillance within the formal working environment has been the norm in various forms over the years. The literature review does demonstrate that before working from home was the norm, surveillance had a number of challenges to worker privacy. However, workers took comfort from the fact, for the most part, they could remove themselves from scrutiny at the end of a shift.

Does employee monitoring impact on workers' right to privacy, while working from home? It is reasonable to conclude that there is an impact, based on the literature research findings and the survey data analysis. The indiscriminate collection of data either passively or deliberately is open to abuse and a breach of trust. The analysis of previous research and the findings of this research paper contribute to a global view that AI and IoT technology are making exciting advances in day-to-day applications. The willingness to invest in this type of technology for financial gain or technological evolution is admirable. But there is also a level of disquiet in society and indeed with developers of this technology that we may have unleashed a digital beast, with unknown consequences due to a lack of oversight and governance. Overall, many will lament the loss of jobs or a reduction in human creativity because of AI technology. The more important aspect to AI, analysed by this paper, is in the context of a workers right to privacy. There is a lack of transparency with an impact on privacy and data security of the

individual and the organisation. No clear road map on ethical behaviour or robust legislation exists thus far.

The value of using remote or lone worker tracking technology in the workplace is undeniable. The implementation of such technology brings numerous advantages, including enhanced employee safety, improved productivity, mitigation of potential risks, cost-effectiveness, and cost avoidance. Through real-time monitoring, immediate assistance during emergencies, streamlined communication, and reduced legal liabilities for health and safety, organisations can create a safer work environment and foster a culture of care for their lone workers. As technology continues to advance, the potential for further enhancements in lone worker tracking systems is vast, offering even greater value to organisations and their employees.

However, advancements in the intelligence of the technology are where it becomes problematic if used for the wrong purposes or dual purposes within a work from home environment. There are significant challenges associated with remote worker tracking systems. The infringement of privacy rights as a direct consequence of gathering personal data should be investigated and monitored. There is a realisation within the EU at least, that in the event of a product failure, current legislation cannot adapt to include AI and IoT under product liability legislation. It appears that product owners and developers can evade responsibility in the event of any type of failure. In turn it could also be argued that the users of AI technology for surveillance, such as employers or their agents would not have responsibility for the algorithms or machine learning behaviour or how or why data would be collected. Transparency in all aspects of the use of all types of remote worker technology is essential. Given the power and speed of the latest AI technology. Ongoing research and recommendations for organisations adopting advanced forms of technology in remote worker tracking should be considered an integral part in the use of AI lone worker tracking technology. As a society, we should seek to harness the power of technology such as AI for the greater good. But this comes at a price, which must be constant review of our codes of ethics, transparency, and all stakeholder interests evaluated. The right to privacy for the end user should remain protected in all instances. The research suggests that there is little evidence or will to enshrine into law the specific right to privacy of a worker while working from home. The findings also conclude that even where there may be a desire to safeguard workers. The pace of technology has so far eluded a requirement to adhere to minimal ethical standards or give workers a credible opportunity to make an informed choice, when looking at remote worker privacy rights in isolation. A light touch self-regulation model falls short of acceptable for the remote worker. There is an attempt to include digital era

governance within 2018 GDPR legislation. Which in itself is no longer fit for purpose. The ethical dilemma of where to draw the line on what is acceptable requires greater oversight and the implementation of a robust framework to protect all. In terms of fairness specifically to the worker from home. At this time, there is zero protective legislation or recourse available to a worker in the event of a breach of trust or indeed breach of privacy rights due to the use of digital remote monitoring. The threat of an invasion of privacy impacting the worker from home is a very real dilemma. It is apparent from the literature review that digital era development has outpaced regulatory oversight and compliance.

Who is watching the watcher. And why is it important to do so? Just because the digital era has created what is arguably so far, the most brilliant of technology in the form of AI and facilitates easier access for society. It doesn't excuse the lack of a mechanism for insuring ethical behaviour, governance and accountability by the owner, developer or user. At the moment there are robust safeguards surrounding employees in terms of health and safety and employment law. The inclusion of a workers right to privacy within the work environment be it onsite or in the home falls short of acceptable, in so far as no specific legislation exists beyond a light touch alignment to GDPR. The researcher does not purport to have expertise in software development, coding or law. Rather a logical and commonsense approach to available research literature and survey analysis. As stated in this paper's introduction, "with great power, comes great responsibility".

References

1.Aloisi, A. and Gramano, E. (2019). Artificial Intelligence Is Watching You at Work.

Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context.

2. Aloisi, A. and DE Stefano, V. (2022) 'Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon', *International Labour Review*,

3. Alsos, K. and Trygstad, S.C. (2023) 'Do participation structures affect workers' voice?', *Economic & Industrial Democracy*, 44(2), pp. 410–431.

4. Atkinson, J. (2018). Workplace Monitoring and the Right to Private Life at Work. *The Modern Law Review*, 81(4), pp.688–700. doi:https://doi.org/10.1111/1468-2230.12357.

5. Awada, M. *et al.* (2021) 'Working from home during the COVID-19 pandemic: Impact on office worker productivity and work experience', *Work*, 69(4), pp. 1171–1189.

6. Ball, K. (2010). Workplace surveillance: an overview. *Labor History*, 51(1), pp.87–106. doi:https://doi.org/10.1080/00236561003654776.

7. Barrick, M. and Mount, M. (1991). The Big Five Personality Dimensions and Job performance: a meta-analysis. *Personnel Psychology*, [online] 44(1), pp.1–26. doi:https://doi.org/10.1111/j.1744-6570.1991.tb00688.x.

8 .Bernhardt, A., Kresge, L. and Suleiman, R. (2023) 'The Data-Driven Workplace and the Case for Worker Technology Rights', *ILR Review*, 76(1), pp. 3–29.

9. .Bogdanović, D. *et al.* (2022) 'Multi-Criteria Analysis of Characteristics of Remote Employee Monitoring Systems', *Proceedings of the International May Conference on Strategic Management*, 18(1), pp. 455–463.

10. Electronic Irish Statute Book (eISB) (2005). *Safety, Health and Welfare at Work Act 2005*. [online] www.irishstatutebook.ie. Available at: https://www.irishstatutebook.ie/eli/2005/act/10/enacted/en/print.

11. Braun, V. and Clarke, V. (2022). Toward Good Practice in Thematic analysis: Avoiding Common Problems and be(com)ing a Knowing Researcher. *International Journal of Transgender Health*, [online] 24(1), pp.1–6. doi:https://doi.org/10.1080/26895269.2022.2129597.

12. Braun, V. and Clarke, V. (2016). (Mis)conceptualising themes, Thematic analysis, and Other Problems with Fugard and Potts' (2015) sample-size Tool for thematic analysis. *International Journal of Social Research Methodology*, [online] 19(6), pp.739–743. doi:https://doi.org/10.1080/13645579.2016.1195588.

13..B. Xia, Q. Lu, L. Zhu, S. U. Lee, Y. Liu and Z. Xing, 'Towards a Responsible AI Metrics Catalogue: A Collection of Metrics for AI Accountability,' 2024 IEEE/ACM 3rd International Conference on AI Engineering – Software Engineering for AI (CAIN), Lisbon, Portugal, 2024, pp. 100-111.. (n.d.).

14. Burrell, G. and Morgan, G. (1983). Sociological Paradigms and Organizational Analysis. *Administrative Science Quarterly*, 28(1), p.153. (Burrell and Morgan, 1983)

15. Carpenter, D., McLeod, A., Hicks, C. and Maasberg, M. (2016). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers*, 20(1), pp.91–110. doi:https://doi.org/10.1007/s10796-016-9667-5.

16. Chesebro, J.W. and Borisoff, D.J. (2007). What Makes Qualitative Research Qualitative? *Qualitative Research Reports in Communication*, 8(1), pp.3–14. doi:https://doi.org/10.1080/17459430701617846.

17. Cloete, F. (2024) 'Governing Artificial Intelligence (AI) and Other Technologies in the Digital Era', *Administratio Publica*, 32(1), pp. 1–30. Available at: https://research.ebsco.com/linkprocessor/plink?id=3872d7e4-119d-36c9-bf2d-b13f24f27977

18. Clover, W.R.L., Francesca Blythe, Arthur (2024). *One Step Closer: AI Act Approved by Council of the EU*. [online] Data Matters Privacy Blog. Available at: https://datamatters.sidley.com/2024/06/06/one-step-closer-ai-act-approved-by-council-of-the-eu/#:~:text=On%2021%20May%202024%2C%20the.

19.Charbonneau, É. and Doberstein, C. (2020) 'An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector', *Public Administration Review*, 80(5), pp. 780–791

20.Centre for International Governance Innovation. (2021). *Privacy in the Precision Economy: The Rise of AI-Enabled Workplace Surveillance during the Pandemic*. [online] Available at: https://www.cigionline.org/articles/privacy-in-the-precision-economy-the-rise-of-ai-enabled-workplace-surveillance-during-the-pandemic/.

21. Collis, J. and Hussey, R. (2014). *Business Research : a Practical Guide for Undergraduate & Postgraduate Students*. 4th ed. Basingstoke: Palgrave Macmillan.

22. Danaher, J. (2020). Freedom in an Age of Algocracy. *The Oxford Handbook of Philosophy of Technology*, pp.249–272. doi:https://doi.org/10.1093/oxfordhb/9780190851187.013.16.

23. Dawson, G.S., Denford, J.S. and Desouza, K.C. (2023). *A cluster analysis of national AI strategies*. [online] Brookings. Available at: https://www.brookings.edu/articles/a-cluster-analysis-of-national-ai-strategies/?utm_campaign=Governance [Accessed 8 Aug. 2024].

24. Das Swain, V., Saha, K., Abowd, G.D. and De Choudhury, M. (2020). Social Media and Ubiquitous Technologies for Remote Worker Wellbeing and Productivity in a Post-Pandemic World. *2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI)*. doi:https://doi.org/10.1109/cogmi50398.2020.00025.

25. Depoy, E. (2016). *Introduction to research : understanding and applying multiple strategies*. Saint Louis, Missouri: Elsevier.

26. digital-strategy.ec.europa.eu. (2023). *Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence | Shaping Europe's digital future*. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-g7-leaders-agreement-guiding-principles-and-code-conduct-artificial.

27. Dentons.com. (2023). *The Future of AI Global Governance*. [online] Available at: https://www.dentons.com/en/insights/articles/2023/july/27/the-future-of-ai-global-governance [Accessed 8 Aug. 2024].

28. Duggan, J., Sherman, U., Carbery, R. and McDonnell, A. (2019). Algorithmic management and app-work in the gig economy: A research agenda for employment relations and HRM. *Human Resource Management Journal*, [online] 30(1), pp.114–132. Available at: https://onlinelibrary.wiley.com/doi/full/10.1111/1748-8583.12258.

29. Dwork, C. and Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3-4), pp.211–407. doi:https://doi.org/10.1561/0400000042.

30. .ECHR (2020). HUDOC - European Court of Human Rights. [online] Coe.int.

31. eela.eelc-updates.com. (n.d.). ECtHR 5 September 2017 (Barbulescu), Applicationno. | EELA Updates.

32. Employer Vehicle Tracking | Data Protection Commission. (n.d.). Employer Vehicle Tracking | Data Protection Commission.

33. European Commission, Joint Research Centre, Ball, K. (2021) *Electronic monitoring and surveillance in the workplace : literature review and policy recommendations*. Publications Office. **https://data.europa.eu/doi/10.2760/5137**

34. European Parliament (2023). EU AI Act: First Regulation on Artificial Intelligence | News | European Parliament.

35. enterprise.gov.ie. (n.d.). *Guidance for working remotely*. [online] Available at: https://enterprise.gov.ie/en/what-we-do/workplace-and-skills/remote-working/#:~:text=Currently%2C%20there%20is%20no%20specific.

36. Fares, N.Y., Nedeljkovic, D. and Jammal, M. (2023). AI-enabled IoT Applications: Towards a Transparent Governance Framework. doi:https://doi.org/10.1109/gcaiot61060.2023.10385106.

37.Fugard, A.J.B. and Potts, H.W.W. (2014). Supporting Thinking on Sample Sizes for Thematic analyses: a Quantitative Tool. *International Journal of Social Research Methodology*, 18(6), pp.669–684.

38.Galanti, T., Ferrara, B., Benevene, P. and Buonomo, I. (2023). Rethinking the Unthinkable: A Delphi Study on Remote Work during COVID-19 Pandemic. *Social sciences*, 12(9), pp.497–497. doi:https://doi.org/10.3390/socsci12090497.

39.Gifford, J. (2022) 'Remote working: unprecedented increase and a developing research agenda', *Human Resource Development International*, 25(2), pp. 105–113. doi:10.1080/13678868.2022.2049108.

40.Groen, B.A.C. *et al.* (2018) 'Managing flexible work arrangements: Teleworking and output controls', *European Management Journal*, 36(6), pp. 727–735.

41.Göndöcs, D & Dörfler, V 2021, 'Post-covid performance management: the impact of remote working experience during the pandemic', Paper presented at 12th IEEE International Conference on Cognitive Infocommunications, 2021, Győr, Hungary, 23/09/21 - 25/09/21 pp. 775-780.

42. Grodzinsky, F.S., Wolf, M.J. and Miller, K.W. (2024). Ethical Issues From Emerging AI Applications: Harms Are Happening. *IEEE Computer*, 57(2), pp.44–52. doi:https://doi.org/10.1109/mc.2023.3332850.

43. Hashim, S., Mohamad, S.F., Abdul Halim Lim, S. and Che Ahmat, N.H. (2022). Pretesting Survey Questionnaire: A Guide on Dissemination. *International Journal of Academic Research in Economics and Management Sciences*, 11(3). doi:https://doi.org/10.6007/ijarems/v11-i3/15228.

44. Harvard Business Review *et al.* (2022) *Hybrid Workplace: The Insights You Need From Harvard Business Review*. Boston, Massachusetts: Harvard Business Review Press. Available at: https://research.ebsco.com/linkprocessor/plink?id=01b79e1f-d621-327e-9b14-8d4d4ac0e5a7

45. Hern, A., (2020), Sep 27. Shirking from home? Staff feel the heat as bosses ramp up remote surveillance. *The Observer*. ISSN 00297712.

46. Hewitt, B. (2023). Panoptic Employment. *The Columbia science and technology law review*, 24(2), pp.349–378. doi:https://doi.org/10.52214/stlr.v24i2.11631.

47. Hickson, J. (2023). Freedom, domination and the gig economy. *New Political Economy*, 29(2), pp.1–16. doi:https://doi.org/10.1080/13563467.2023.2254712.

48. Hillman, J. (2023) 'Smart Regulation: Lessons from the Artificial Intelligence Act', *Emory International Law Review*, 37(4), pp. 775–826. Available at: https://research.ebsco.com/linkprocessor/plink?id=d6ce6c84-67e3-3942-8392-b80904078a70 (Accessed: 6 August 2024).

49.Home of internet privacy. (2021). *ExpressVPN Survey Shows Widespread Surveillance on Remote Workers*. [online] Available at: https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/.

50. Hughes, C., Robert, L., Frady, K. and Arroyos, A. (2019). Artificial Intelligence, Employee Engagement, Fairness, and Job Outcomes. *Managing Technology and Middle- and Low-skilled Employees*, pp.61–68. doi:https://doi.org/10.1108/978-1-78973-077-720191005.

51.Jandl, C. *et al.* (2021) 'Reasons and Strategies for Privacy Features in Tracking and Tracing Systems-A Systematic Literature Review', *Sensors (Basel, Switzerland)*, 21(13).

52. Kaduk, A., Genadek, K., Kelly, E.L. and Moen, P. (2019). Involuntary vs. voluntary flexible work: insights for scholars and stakeholders. *Community, Work & Family*, 22(4), pp.412–442. doi:https://doi.org/10.1080/13668803.2019.1616532.

53. Katsabian, T. (2023) 'The Telework Virus: How COVID-19 Has Affected Telework and Exposed Its Implications for Privacy', *Berkeley Journal of Employment & Labor Law*, 44(1), pp. 141–190. doi:10.15779/Z38QF8JK7H.

54. Kalish, L. (2022). A Silicon Valley lawmaker wants to protect workers from employer spying. *CalMatters*. [online] 19 Apr. Available at: https://calmatters.org/california-divide/2022/04/california-workers-surveillance/.

55. Ka Manoj Kumar, M Madhu, Br Pratyaksha, S Sushmita and Javed, G.S. (2023). Ethical AI Conundrum: Accountability and Liability of AI decision making. doi:https://doi.org/10.1109/temscon-aspac59527.2023.10531445.

56. Keane, E. (2018). The GDPR and Employee's Privacy: Much Ado but Nothing New. *King's Law Journal*, 29(3), pp.354–363. doi:https://doi.org/10.1080/09615768.2018.1555065.

57. Kellogg, K.C., Valentine, M.A. and Christin, A. (2020). Algorithms at Work: The New Contested Terrain of Control. *Academy of Management Annals*, 14(1), pp.366–410.

58. Ketelaar, P.E. and van Balen, M. (2018) 'The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking', *Computers in Human Behavior*, 78, pp. 174–182.

59. Kritikos, M. (2023). Surveillance and the Modern Workplace. *Advances in research ethics and integrity*, pp.1–4. doi:https://doi.org/10.1108/s2398-601820230000010001. (Kritikos, 2023)

60. Kritikos, M. and Iphofen, R. (2023). Draft and Develop an Ethical Charter/Governance Framework. *Advances in research ethics and integrity*, pp.71–72. doi:https://doi.org/10.1108/s2398-601820230000010030.

61. Kritikos, M. and Iphofen, R. (2023). Misuse/Dual Use. *Advances in research ethics and integrity*, pp.87–87. doi:https://doi.org/10.1108/s2398-601820230000010038. (Kritikos and Iphofen, 2023)

62. Krzywdzinski, M., Gerst, D. and Butollo, F. (2022). Promoting human-centred AI inthe workplace. Trade unions and their strategies for regulating the use of AI in Germany. Transfer: European Review of Labour and Research,

63. www.legal-island.ie. (n.d.). *Surveillance of Employees in Ireland - Protecting Employee Rights in the New Digital Age*. [online] Available at: https://www.legal-island.ie/articles/ire/features/supplementary/2023/july/surveillance-of-employees-in-ireland---protecting-employee-rights-in-the-new-digital-age/.

64.Lincoln, Y.S. and Denzin, N.K. (2009). Handbook of Qualitative Research : Norman K. Denzin, Yvonna S. Lincoln.

65. Luna, A. *et al.* (2022) 'Proposed Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks', *2022 IEEE High Performance Extreme Computing Conference (HPEC), High Performance Extreme Computing Conference (HPEC), 2022 IEEE*, pp. 1–2.

66. The Irish Congress of Trade Unions. (n.d.). Artificial Intelligence in the workplace -Dr. Laura Bambrick.

67. Madiega, T. (2023). *BRIEFING EU Legislation in Progress Proposal for a directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence (AI liability directive) Ordinary legislative procedure (COD) (Parliament and Council on equal footing - formerly 'co-decision')*. [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

68. Mark (2023). *Privacy in the Age of AI: Risks, Challenges and Solutions*. [online] Dr Mark van Rijmenam, CSP | Strategic Futurist Speaker. Available at: https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/#:~:text=As%20AI%20technology%20advances%2C%20the [Accessed 19 Aug. 2024].

69. Mason Hayes Curran. (2024). *The AI Act is Adopted: Compliance Obligations on the Horizon*. [online] Available at: https://www.mhc.ie/latest/insights/the-ai-act-is-adopted-compliance-obligations-on-the-horizon [Accessed 19 Aug. 2024].

70. McKendrick, J. and Thurai, A. (2022). *AI Isn't Ready to Make Unsupervised Decisions*.

71. Montreuil, S. and Lippel, K., 2003. Telework and occupational health: a Quebec empirical study and regulatory implications. *Safety Science*, *41*(4), pp.339-358.

72. Moore, B. (2024). What competencies will be needed to manage Artificial Intelligence in the workplace? (An AI perspective). *Assessment & Development Matters*, [online] 16(1), pp.4–8. doi:https://doi.org/10.53841/bpsadm.2024.16.1.4.

73. Morgan, K. and Nolan, D. (2023). *How worker surveillance is backfiring on employers*. [online] www.bbc.com. Available at: https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers.

74. Morley, N. (2022) 'Employee Engagement Data and Performance Parameters, Algorithmic Tracking and Remote Workplace Technologies, and Interoperable Virtual Networks in the Decentralized and Interconnected Metaverse', *Psychosociological Issues in Human Resource Management*, 10(2).

75. Nassaji, H. (2020). Good Qualitative Research. *Language Teaching Research*, [online] 24(4), pp.427–431. Available at: https://journals.sagepub.com/doi/full/10.1177/1362168820941288.

76. Nissenbaum, H. (2009). *Privacy in Context*. Stanford University Press.

77.Olsen, M. (2019) 'Using Data Analytics in the Management of Employees: Digital Means of Tracking, Monitoring, and Surveilling Worker Activities', *Psychosociological Issues in Human Resource Management*, 7(2), p. 43.

78. Ozatay, M., Aygun, L., Jia, H., Kumar, P., Mehlman, Y., Wu, C., Wagner, S., Sturm, J. and Verma, N. (n.d.). *Artificial Intelligence Meets Large-Scale Sensing: using Large-Area Electronics (LAE) to enable intelligent spaces*. [online] Available at: https://www.princeton.edu/~nverma/VermaLabSite/Publications/2018/OzatayAygunJiaKumarMehlmanWuWagnerSturmVerma_CICC2018.pdf

79. Palagolla, N. (2016). Exploring the Linkage between Philosophical Assumptions and Methodological Adaptations in HRM Research. *Journal of Strategic Human Resource Management*, 5(1). doi:https://doi.org/10.21863/jshrm/2016.5.1.020.

80. Pieroni, B. (2024) 'The Impact of Tech: How AI Is Already Transforming Our Industry: Emerging AI solutions enable a machine to "understand" rather than simply reproduce data', *Best's Review*, 1 June. Available at: https://research.ebsco.com/linkprocessor/plink?id=a3dd8f97-2747-3fa5-8aca-6db9587f9005

81. Ponterotto, J. (2015). Brief Note on the Origins, Evolution, and Meaning of the Qualitative Research Concept Thick Description. *The Qualitative Report*, 11(3). doi:https://doi.org/10.46743/2160-3715/2006.1666.

82. Presbitero, A. and Teng-Calleja, M. (2022). Job attitudes and career behaviors relating to employees' perceived incorporation of artificial intelligence in the workplace: a career self-management perspective. *Personnel Review*, 52(4), pp.1169–1187. doi:https://doi.org/10.1108/pr-02-2021-0103.

83. Presser, S., Rothgeb, J.M., Comper, M.P., Lessler, J.T., Martin, E., Martin, J. and Singer, E. (2005). Review of Methods for Testing and Evaluating Survey Questionnaires. *BMS: Bulletin of Sociological Methodology / Bulletin de Méthodologie Sociologique*, [online] (87), pp.89–89. Available at: https://www.jstor.org/stable/23931305 [Accessed 29 Jul. 2024].

84. Princi, E. and Krämer, N. c. (2019). Acceptance of smart electronic monitoring atwork as a result of a privacy calculus decision. *Informatics*, [online] 6(3). doi:https://doi.org/10.3390/informatics6030040.

85. Ravid, D.M., Tomczak, D.L., White, J.C. and Behrend, T.S. (2019). EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management*, 46(1), pp.100–126. doi:https://doi.org/10.1177/0149206319869435.

86. Robert, L.P., Pierce, C., Marquis, L., Kim, S. and Alahmad, R. (2020). Designing fair AI for managing employees in organizations: a review, critique, and design agenda. *Human–Computer Interaction*, 35(5-6), pp.1–31. doi:https://doi.org/10.1080/07370024.2020.1735391.

87. Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review*, 34(1), pp.99–110. doi:https://doi.org/10.1016/j.clsr.2017.05.021.

88. Sahay, A. (2016). *Peeling Saunder's Research Onion*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/309488459_Peeling_Saunder.

89.Sanderson, C., Schleiger, E., Douglas, D., Kuhnert, P. and Lu, Q. (2024). Resolving Ethics Trade-offs in Implementing Responsible AI. doi:https://doi.org/10.1109/cai59869.2024.00215.

90 .Saunders, M., Lewis, P., Thornhill, A. and Bristow, A. (2019). *'Research Methods for Business students' Chapter 4: Understanding Research Philosophy and Approaches to Theory Development*.

91. Saunders, M., Lewis, P., Thornhill, A. and Bristow, A. (2019). *'Research Methods for Business students' Chapter 4: Understanding Research Philosophy and Approaches to Theory Development*.

92. Schoenherr, J.R. *et al.* (2023) 'Designing AI Using a Human-Centered Approach: Explainability and Accuracy Toward Trustworthiness', *IEEE Transactions on Technology and Society, Technology and Society, IEEE Transactions on, IEEE Trans. Technol. Soc*, 4(1), pp. 9–23.

93.Siegel, R., König, C.J. and Lazar, V. (2022). Impact of electronic monitoring on employees: A meta-analysis. *Computers in Human Behavior Reports*, [online] 8, p.100227. doi:https://doi.org/10.1016/j.chbr.2022.100227.

94. Schmauder, C., Karpus, J., Moll, M., Bahrami, B. and Deroy, O. (2023). Algorithmic Nudging: The Need for an Interdisciplinary Oversight. *Topoi*, [online] 42(3), pp.799–807. doi:https://doi.org/10.1007/s11245-023-09907-4.

95. Schneider, D. and Weber, K. (2024). AI for decision support: What are possible futures, social impacts, regulatory options, ethical conundrums and agency constellations? *Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 33(1), pp.8–54. doi:https://doi.org/10.14512/tatup.33.1.08.

96. Solove, D. J. The Limitations of Privacy Rights. **Notre Dame Law Review**, *[s. l.]*, v. 98, n. 3, p. 975, 2023.

97. Stark, L., Stanhaus, A. and Anthony, D.L. (2020). 'I Don't Want Someone to Watch Me While I'm Working': Gendered Views of Facial Recognition Technology in Workplace Surveillance. *Journal of the Association for Information Science and Technology*, 71(9). doi:https://doi.org/10.1002/asi.24342.

98. Stone, E.F., Gueutal, H.G., Gardner, D.G. and McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), pp.459–468. doi:https://doi.org/10.1037/0021-9010.68.3.459.

99. Survey Results link: https://bit.ly/4dMugrh

100. Taylor, B. and Francis, K. (2013). *Qualitative Research in the Health Sciences*. Routledge. doi:https://doi.org/10.4324/9780203777176.

101. The Century Foundation. (2018). *The Datafication of Employment*. [online] Available at: https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?agreed=1 [Accessed 29 Mar. 2020].

102. Thiel, C.E., MacDougall, A.E. and Bagdasarov, Z. (2019). Big (Benevolent) Brother. *Organizational Dynamics*, 48(2), pp.19–28.

103. Tjano, Robert. (2023). CHAPTER 5: THE RESEARCH DESIGN AND METHODOLOGY. (n.d.).

104.Torres, S. and Orhan, M.A. (2023) 'How it started, how it's going: Why past research does not encompass pandemic-induced remote work realities and what leaders can do for more inclusive remote work practices', *Psychology of Leaders and Leadership*, 26(1), pp. 1–21.

105. Tsvetkov, K. (2023) 'How Did Infomatics Begin?', *New Knowledge Journal of Science / Novo Znanie*, 12(2), pp. 37–47. Available at: https://research.ebsco.com/linkprocessor/plink?id=1a996f32-9462-357a-990b-20c701fbdf3c (Accessed: 14 August 2024).

106. Urbane, M. (2023). The impact of digitalization on the working time in the EU: legal considerations of the right to disconnect. doi:https://doi.org/10.1109/icte58739.2023.10488586.

107. V. Dankan Gowda, Kaur, M., Srinivas, D., Prasad, V. and R. Shekhar (2024). AIoT Integration Advancements and Challenges in Smart Sensing Technologies for Smart Devices. *Advances in computational intelligence and robotics book series*, pp.42–65. doi:https://doi.org/10.4018/979-8-3693-0786-1.ch003.

108. Vitak, J. and Zimmer, M. (2023). Surveillance and the future of work: exploring employees' attitudes toward monitoring in a post-COVID workplace. *Journal of Computer-Mediated Communication*, 28(4). doi:https://doi.org/10.1093/jcmc/zmad007.

109. Vitak, J. and Zimmer, M. (2023). Power, Stress, and Uncertainty: Experiences with and Attitudes toward Workplace Surveillance During a Pandemic. *Surveillance & Society*, 21(1), pp.29–44. doi:https://doi.org/10.24908/ss.v21i1.15571.

110. Wheeler, T. (2023). *The three challenges of AI regulation*. [online] Brookings. Available at: https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/?utm_campaign=Center

111.Wolf, C.W. and F. (2010). Telework in the European Union. *policycommons.net*. [online] Available at: https://policycommons.net/artifacts/1834407/telework-in-the-european-union/2576407/

112. Yerby, J. (2013). *(PDF) Legal and ethical issues of employee monitoring*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/313656700_Legal_and_ethical_issues_of_employee_monitoring.

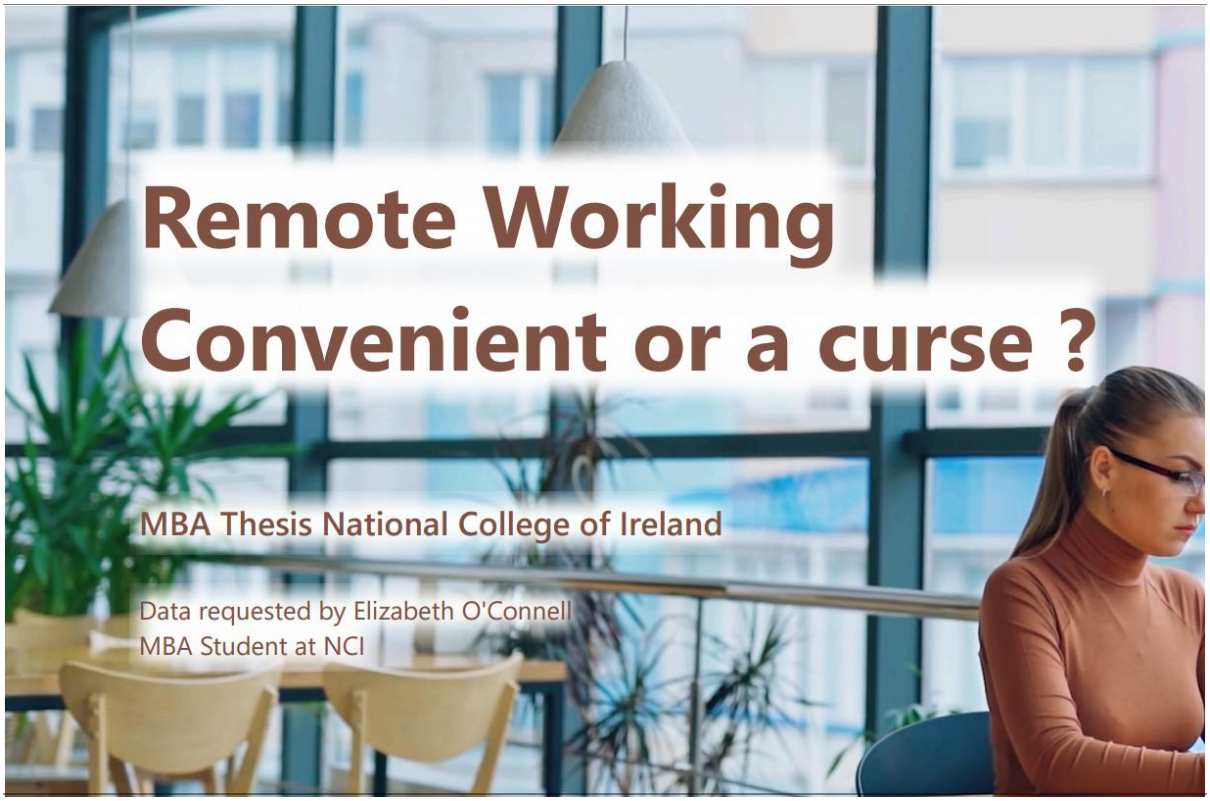
113. Zhang, H., Lee, S., Lu, Y., Yu, X. and Lu, H. (2022). A Survey on Big Data Technologies and Their Applications to the Metaverse: Past, Current and Future. Mathematics, 11(1), p.96.

114. Zanker, M. *et al.* (2021) 'The Gdpr at the Organizational Level: A Comparative Study of Eight European Countries', *E+M Ekonomie a Management*, 24(2).

115. Zheng, X., Cai, Z. and Li, Y. (2018). Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective. *IEEE Communications Magazine*, 56(9), pp.55–61. doi:https://doi.org/10.1109/mcom.2018.1701245.

116. Zuboff, S., 2023. The age of surveillance capitalism. In *Social theory re-wired* (pp. 203-213). Routledge.

Appendix 1



The survey is exploring the impact of monitoring on remote workers privacy.

Please avoid providing Yes, No or N/A answers. All data is anonymised.

1.How do you feel about employee monitoring while working remotely?

2.Do you think there is enough transparency surrounding the type of monitoring technology used, especially with advancements in technology?

3.Does it concern you that monitoring may impact your privacy?

4.Have you ever requested additional information on the type and purpose of monitoring software?

5.If you were concerned about the use of monitoring software or purpose, do you feel you could raise this with an Employer?

6.Would you be concerned that monitoring software may imply a lack of trust by an employer or a sense that your work ethic is in question? If you had a choice, would you agree to remote monitoring technology?

Appendix 2

Information Sheet

Thank you for considering participating in this research project. This document is to explain to you what the work is about and what your participation would involve, so as to enable you to make an informed choice.

The purpose of this study is to research the impact of monitoring technology on remote workers. My thesis research question seeks to establish whether monitoring of remote workers using technology infringes on a worker right to privacy. Should you choose to participate, you will be asked to participate in a survey delivered via a Microsoft Forms link. You will be asked to complete a questionnaire, which will include questions on your experiences or awareness of remote worker monitoring technology. However, there are no right or wrong answers as the questions are open ended and responses are unique to the participant. Clarification may be sought from the researcher.

Participation in this study is completely voluntary. There is no obligation to participate, and should you choose to do so, you can refuse to answer specific questions or decide to withdraw from the study. All information you provide will be confidential and participation will be anonymous.

You maintain the right to withdraw from the study at any stage up to the point of data submission. At this point your data will be collated with that of other participants and can no longer be retracted.

Thank you.

Survey Participation Consent Form

Researcher: Elizabeth O'Connell

Status: Student of National College of Ireland

Study Program: MBA

Contact Details: x21138915@student.ncirl.ie and lizoconnell2017@gmail.com and 086 8240097

The anonymous survey data will be stored on my student account OneDrive with The National College of Ireland and a local hard drive. Collated data including information submitted on the survey will be used to form part of my conclusions on my finished thesis.

Submission of the completed survey implies consent to participate in this study? Terms of participation are as outlined in the information sheet.

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form
(Thesis/Author Declaration Form)

Name: Elizabeth O'Connell_

Student Number: 21138915

Degree for which thesis is submitted: Masters in Business Administration

Title of Thesis: Does employee monitoring infringe on workers' right to privacy, while working from home?

Thesis supervisor: Professor Paul Hanly

Date: 27th August 2024

Material submitted for award

A. I declare that this work submitted has been composed by myself. Yes

B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged. Yes

C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA. Yes

D. ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award.

_____

I declare that no material contained in the thesis has been used in any other submission for an academic award.