Boss is aWare—Are you? Employee Comprehension and Legal Awareness of Workplace Monitoring

Teshan S. Bunwaree
School of Computer Science and Informatics
Cardiff University
Cardiff, Wales, UK
BunwareeTS@cardiff.ac.uk

Katarzyna Stawarz
School of Computer Science and Informatics
Cardiff University
Cardiff, Wales, UK
StawarzK@cardiff.ac.uk

Philippa Collins
Law School
University of Bristol
Bristol, England, UK
philippa.collins@bristol.ac.uk

Sandy J.J. Gould
School of Computer Science and Informatics
Cardiff University
Cardiff, Wales, UK
goulds@cardiff.ac.uk

ABSTRACT

Bossware, software that monitors worker activity, is a common feature of workplaces. What do workers know about these tools and how they relate to their rights at work? We explored this question through two studies. Study 1 surveyed 100 workers to assess their understanding of work monitoring terminology. Participants were confident in their knowledge of key terms but struggled to accurately define them. Study 2 explored awareness of legal protection in relation to work monitoring through 19 semi-structured online interviews. We found that awareness varied with industry and work role, but was generally low and lacked certainty. Participants were largely skeptical of the use of bossware, questioning its necessity. Limited knowledge of monitoring terminology and legal protection at work further weakens workers' ability to notice and challenge the use of monitoring tools in their workplaces. We finish by speculating on whether educating workers about bossware and workplace rights would help.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**; • **Social and professional topics → Employment issues**.

KEYWORDS

bossware, work monitoring, surveillance, tracking, privacy

ACM Reference Format:
Teshan S. Bunwaree, Katarzyna Stawarz, Philippa Collins, and Sandy J.J. Gould. 2025. Boss is aWare—Are you? Employee Comprehension and Legal Awareness of Workplace Monitoring. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3706598.3713651

CHI '25, April 26-May 1, 2025, Yokohama, Japan

1 INTRODUCTION

The use of software designed to monitor and manage employees has grown in popularity over the last few years, particularly in response to the rise of remote work as the predominant mode of working [44]. Often marketed as Electronic Performance Monitoring (EPM) tools, Work Monitoring Software (WMS), or instead referred to as "Bossware" by some, these systems enable employers to track employee performance at scale, which can even be done without the employee's knowledge or consent. These tools utilize methods such as keylogging software, screen capture features, mouse movement tracking, email and call monitoring, internet webpage access monitoring, and face recognition software [3, 6, 7, 21, 23, 37, 38, 66, 73]. Beyond software, physical devices like IoT sensors (e.g., GPS, RFID), wearables (e.g., smartwatches or fitness trackers), and cameras (e.g., CCTV or webcams) are also employed in employee surveillance [34, 67]. The visibility of these surveillance practices can vary, with some being overt while others remain hidden, depending on the features of the specific software or devices used [3, 23].

High-profile cases have highlighted the controversial nature of such surveillance practices. For instance, Barclays faced backlash in 2020 after using Sapience Analytics' software, which prompted employees with productivity tips and monitored their activities without their knowledge, leading to the cessation of its use [50]. Similarly, both Barclays and The Daily Telegraph encountered criticism for using OccupEye, a monitoring solution designed to track office space usage through motion and heat sensors, which was eventually withdrawn due to negative reactions from employees who felt their presence at their desks was being closely monitored [25, 47, 65].

The management and psychological literatures have reported negative effects associated with intensive work monitoring practices, including worsening work performance and wellbeing, and the emergence of counterproductive work behaviors [45, 46, 51]. Legal scholars have criticized the way companies justify their intrusive monitoring practices and have highlighted the employee-employer power differential, which often prevents employees from having their concerns considered before such practices are implemented [7, 20]. Human-Computer Interaction (HCI) research has kept up with advances in workplace monitoring technology, exploring the potential privacy and ethical issues arising from the collection of sensitive data [53, 68, 69]. However, employees' understanding of work monitoring and its legal frameworks have received less attention.

Collins [19] identified a split between legal and technical spheres which highlights how algorithmic management systems, which include bossware, create challenges due to their technical opacity (e.g., complexity and trade secrets) and legal barriers to transparency and accountability. This disconnect hinders workers' ability to understand, challenge, or influence these systems effectively. Information asymmetry arises where an employer holds more information about the managerial systems in place compared to employees. This leads to a situation which is inherently unfair to employees, as they are not equipped to challenge the systems which monitor them [19, 22, 29]. Pleger et al. [64] have previously shown that UK citizens lacked understanding of data protection and data security, despite them indicating medium to high levels of familiarity with various terms related to data protection and data security. This assumes that the employer has more knowledge over matters of workplace monitoring and data protection compared to employees, however, it could be the case that even employers might not be well-informed in terms of emerging legal compliance with regard to data protection. In the early days of the implementation of the GDPR in the UK in 2018, Addis and Kutar [1] had shown how UK companies exhibited low levels of awareness with respect to the regulations. They also found low levels of knowledge about changes to the data protection landscape, and it was apparent even at the executive level. The implementation of technologies within the workplace should be accompanied by the relevant legal compliance as well as efforts by management in educating employees and also themselves about the matter. A survey of 719 leaders of small businesses in 2019 reported that nearly half of respondents admitted to their business failing at key compliance components of the GDPR [30]. Furthermore, the leaders were confused about basic data security concepts such as encryption. We need to consider that it is more likely for larger companies to tackle the process of informing the company to a satisfactory degree, as they have more resources to allocate to ensure compliance with data protection laws and train employees [71]. Small and medium enterprises may not have the same resources for and focus on data protection.

As seen above, previous work has focused directly on individuals' perspectives on data protection and the GDPR. This paper looks into employees' views towards work monitoring, in particular their awareness of the topic and its legal frameworks. It is imperative to have individuals be literate about work monitoring practices and the law surrounding it, as the extent to which employees can question and challenge monitoring may likely be influenced by their collective knowledge and understanding [9, 19, 22]. For one, a lack of challenge to monitoring practices could lead to employers' policies falling short of protecting individual rights. Through this exploratory research, we assess employees' knowledge of work monitoring practices and note their expectations about the law. While the accuracy of knowledge of employees is a metric in assessing this, it is not the purpose of this paper to make claims solely based on the accuracy of their knowledge – rather we seek to lay out the quality of their knowledge in how they choose to express their knowledge. The findings will allow us to report on the current state of employees' knowledge on the matter of monitoring at work. This benchmarking is an essential starting point for the applied context of supplementing current data protection guidance and training in workplaces, and also for academic research projects examining perspectives on workplace surveillance.

2 RELATED WORK

There are three key reasons why employers monitor their employees: ensuring adherence to contract agreements and compliance with company policies and expectations, managing legal liabilities, and protecting against security breaches [52, 54]. Monitoring helps in assessing productivity and preventing misconduct, which, the theory goes, translates into business success. Historically, the modern concept of work monitoring originates from Scientific Management, pioneered by Frederick Taylor in the early 1900s. Taylor's framework involved breaking down tasks into smaller components for efficiency assessment, initially applied to factory workers performing repetitive manual tasks [33, 74, 75]. In modern work roles, across industries, at larger scales, and especially in remote work contexts, this type of direct monitoring is not feasible. While it is conceivable that, say, one manager can be in charge of a small team of five people while having good idea of the productivity of their team members individually, the same cannot be said about a human managing hundreds or thousands of employees all at once over a myriad of tasks [3]. Monitoring through digital solutions can handle (or purports to handle) this large-scale task, hence the emergence of Bossware.

2.1 Arguments For Bossware

Bossware, or employee monitoring software, has been used for decades and has both proponents and critics. Supporters argue that Bossware can enhance employee performance and bring objectivity to evaluations [2, 10, 11, 14, 55]. Aiello and Kolb's study on 202 undergraduate Psychology students demonstrated that Electronic Performance Monitoring (EPM) improved performance on simple tasks but hindered it on complex ones [2]. This pattern aligns with social facilitation theory, which holds that performance on individual tasks is improved when in the presence of others [78]. High-performing participants showed further improvement with EPM, whereas low performers exhibited reduced performance. However, the results should be viewed in context, as they are based on university students and may not reflect the general working population.

Interestingly, the reception of Bossware can vary depending on how it is framed by employers. Some employees may view monitoring negatively, but others might accept it as a way to demonstrate their productivity or feel secure, as seen in studies involving call center workers and other employees [70, 72]. When monitoring practices are framed as tools for employee development rather than as behavioral deterrents, they can lead to greater job satisfaction and organizational commitment [77]. Thus, the strategic introduction of Bossware, with an emphasis on its benefits for employees, can potentially foster a more positive response to electronic monitoring.

2.2 Arguments Against Bossware

Despite potential performance benefits, substantial evidence highlights negative effects of surveillance. Research indicates that electronic monitoring can negatively impact worker attitudes and trust [5, 11, 17]. Jeske [43] noted that while workplace surveillance tools might enhance communication and support self-development if employees have access to their performance data, excessive monitoring can damage trust and lead to lower perceptions of trust in management for employees [35, 43]. Privacy intrusion is a general concern when considering monitoring software, and it has been found to be felt deeply by employees in the case of emotion AI (measuring employees' emotions and mood) being used in monitoring software [68]. Intensive monitoring has also been linked to decreased organizational citizenship, reduced employee performance, and lower overall well-being [45]. In the case of gigworkers, surveillance at work led to feelings of their privacy, safety, and economic outcomes being threatened [69].

Bossware can also prompt employees to engage in counterproductive work behaviors (CWBs), such as avoiding monitored areas or using 'mouse jigglers' to simulate activity [16, 51, 76]. Some other examples of CWBs include spending time browsing the internet or taking personal phone calls during work hours, avoiding monitored areas, intentionally working slowly, and taking unnecessarily long breaks. Some of these practices may undermine the accuracy of monitoring software, and thus highlights a critical flaw in relying solely on machine measurement for employee monitoring purposes.

2.3 Legal Considerations

We focus on the UK context in this paper, as each jurisdiction has its own set of laws which govern issues of data protection and employment rights. There are three main pillars which govern workplace monitoring: data protection, human rights and employment law. Article 8 of the European Convention on Human Rights (ECHR)[27] incorporated into UK law by the Human Rights Act (HRA) 1998 confers the right to respect for private and family life [62]. The Data Protection Act (DPA) 2018 and the UK General Data Protection Regulations (GDPR) regulate personal data processing, with the GDPR outlining principles for lawful data handling: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability [28, 63]. Following Brexit, the EU GDPR was retained into UK law as the UK GDPR which is enshrined into UK law by the DPA 2018. The EU GDPR's key principles, rights and obligations remain the same in the UK version, and the UK has the independence to keep the framework under review [40].

Non-compliance with the UK GDPR principles can result in significant penalties equivalent to "£17.5 million or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher" [39, 63]. As for Employment law, the relevant legislation is the Employment Rights Act 1996 which does not directly address work monitoring or surveillance [61]. However, it provides a general framework for fair treatment in the workplace such as the right to not be unfairly dismissed, which indirectly relates to monitoring in certain contexts.

The dominant pieces of legislation in matters of work monitoring, and the ones we will be referring to most throughout this research, are the DPA 2018 and the UK GDPR. Employers must adhere to two key requirements under the GDPR: data protection principles and lawful bases for processing personal data. As per Art.5 of the UK GDPR, the seven key principles are as follows: data must be processed lawfully, fairly, and transparently (Lawfulness, Fairness, and Transparency); collected for specific, legitimate purposes (Purpose Limitation); limited to what is necessary (Data Minimisation); accurate and up to date (Accuracy); kept no longer than necessary (Storage Limitation); securely processed to ensure confidentiality (Integrity and Confidentiality, or security); and organizations must be able to demonstrate compliance (Accountability) [63].

Art.6 of the UK GDPR allows for employee monitoring only if one of the following lawful bases is shown to be applicable: (a) consent, (b) contract necessity, (c) legal obligation, (d) vital interests, (e) public task, and (f)legitimate interests [36, 63]. Bases (d) and (e) are unlikely to apply to processing for bossware purposes, we can therefore consider in more detail how the remaining bases apply in the bossware context.

In the case of (a) consent, "the data subject has given consent to the processing of his or her personal data for one or more specific purposes", it is possible to rely on it as a lawful basis. Where the worker has given consent to have their personal data processed by the employer for the purpose of monitoring, consent may be relied upon as a lawful basis. However, this lawful basis is only valid where the employee is in a position to freely give their consent. In an employment context, there is an inherent power difference between the two parties and so it would only be appropriate to rely on consent as a lawful basis where the employee can expect no negative consequences as a result of refusing to consent to the monitoring [36]. As for (b) contract, "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract", the processing of data from work monitoring is necessary for a contract to exist between the worker and employer, or because the worker requested specific conditions from the employer such as e.g. remote working arrangements. Regarding (c) legal obligation, where "processing is necessary for compliance with a legal obligation to which the controller is subject", the processing of personal data is necessary for the employer to comply with the law e.g. in the case of monitoring to ensure compliance with Health and Safety laws and anti-fraud measures as per financial regulations. Finally, the UK GDPR holds for a lawful basis of (f) legitimate interests that the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." Where the processing of personal data is necessary for the employers' legitimate interests or those of a third party, unless the risks to the workers rights overrides them. Relying on legitimate interests requires satisfying three tests: purpose, necessity, and balancing; Is there a legitimate interest in processing the personal data? Is the processing necessary for that purpose? Is the legitimate interest overridden by the worker's interests, rights, or freedoms [28, 63]?

The context of remote work and Bossware raises concerns about potential infringements of Art. 8 HRA [48]. Academics caution against companies presenting surveillance as compliant with data protection principles without addressing underlying legal issues [6, 20, 57]. Companies might frame surveillance as necessary for business efficiency [8] and while practices exceeding lawful boundaries can be contested by employees or their trade union representative, this is unlikely to be feasible in practice [20, 22]. Collins and Marassi [20] maintain that unreasonable surveillance practices which do not fall strictly within the conditions for lawfulness in the GDPR can be challenged. They also suggest that to reduce imbalances in power that may arise between employee and employer, employees should be part of the conversation at early stages of decision-making for the implementation of monitoring practices and data management.

To summarise, bossware is legal in the UK, but it is also tightly regulated under the Data Protection Act 2018 (including the UK GDPR), the Human Rights Act 1998, and employment law. Employers must have a lawful basis for monitoring, such as legitimate interest, and comply with principles of fairness, transparency, and necessity. The Human Rights Act protects employees' right to privacy, requiring monitoring to be proportionate and justified. Employment law mandates that monitoring aligns with workplace policies and contracts, with clear communication to employees. Breaches of these laws can result in penalties, emphasizing the need for careful and responsible use of monitoring tools. For the purpose of this research, we choose to largely focus on the DPA 2018 and UK GDPR as these are the key legal frameworks governing work monitoring practices.

2.4 Research Gap and Contribution

This research aims to bridge individual experiences of work, organizational structures, technology, and the law, addressing a critical gap in prior work that has often treated these elements in isolation. By taking an integrative approach towards these domains, we seek to highlight the complex interplay between these factors and contribute to the literature by exploring workers' experiences and knowledge on the matter.

Discussions about the link between the technical and legal have been scarce in relation to bossware. The technical is dependent on multiple factors, some of which are in the control of bossware providers and their clients, company management. As for the legal side, data protection legislation has been established for years now, yet employee, and even employer, understanding on the matter has been shown to be lacking [22]. This disconnect between legal frameworks and technical systems highlights how complex algorithmic management tools, as is the case in bossware, can outpace regulatory oversight, limiting transparency, accountability, and workers' ability to challenge their use effectively [19]. This research has for objective to contextualize this split between the technical and legal by taking the approach of assessing the employee's experience and knowledge.

Existing literature addresses psychological, managerial, and legal aspects of Bossware, though a notable gap exists in our understanding of employees' awareness and interpretation of work monitoring terms and legal protections. Developing this knowledge would be greatly beneficial for reviewing how we are currently educating employees about their rights at work, especially in the data protection context, with GDPR training being offered in some industries. Through this investigation, we will be able to highlight what employees know and assume of the law, which will then be useful for reviewing how we educate employees on the matter. Finally, the information gathered here will serve to better design research to account for discrepancies in employee knowledge of work monitoring practices.

This paper presents two empirical investigations into workplace monitoring. Study 1, an online survey, seeks to answer the question of how well-versed employees are about work monitoring terminology. Study 2, through semi-structured online interviews, explores the level of legal awareness employees have regarding work monitoring practices. The aim of this research is to explore the state of employee knowledge regarding work monitoring practices and its legality rather than strictly measuring employees' knowledge.

3 STUDY 1: ONLINE SURVEY

Study 1, conducted as an online survey, investigated workers' familiarity with, and substantive understanding of, workplace monitoring terminology.

3.1 Context

This study focused on the United Kingdom, where all authors are based, to account for its specific legal and regulatory environment governing workplace monitoring practices. The post-Brexit adoption of the GDPR into UK law alongside the UK Data Protection Act 2018 shape the legal framework for employee rights and employer obligations. By grounding the research in the UK context, this study aims to provide insights that are directly applicable to UK-based workers. However, these may also contribute to broader discussions about work monitoring practices across other populations and legal jurisdictions.

3.2 Rationale

It is unclear what researchers, HR professionals, trade unions, legislators, educators and other interested parties might assume when engaging with workers on this topic. There is a risk that familiarity might be confused with a substantive understanding. For example, expectations that being familiar with the term "GDPR" would be taken to mean that someone has a functional understanding that they can use to make sense of the monitoring in their workplace. The consequences of talking at cross purposes might be that workers are not able to exercise their rights at work, that employers unwittingly breach those rights, or that tools designed to support workers and their representatives do not have the anticipated effect.

We examined participants' self-ratings of familiarity with eight terms and compared these ratings with their definitions of the terms, which we evaluated quantitatively against baseline definitions. We also performed a thematic analysis to understand the qualitative aspects of their understanding. Lastly, we gauged how much employees cared about the topics associated with the terms through sets of attitudinal questions, however, these will not be reported in this paper.

3.3 Method

3.3.1 Participants and Recruitment. This exploratory study was conducted in May 2023. UK-based participants were recruited to ensure that participants had a similar experience regarding data protection and employment laws. Prolific, a platform for recruiting participants, was used to recruit 100 adult UK residents who were fluent in English and had experience working in-office, remotely, or both. The sample target was set at 100 participants which we deemed sufficient for the purposes of this study, given its exploratory nature and that our goal was to understand cohort understanding across the definitions, rather than to investigate relative differences in the levels of understanding of the terms [1]. Following Prolific's standard guidelines, participants were remunerated at a rate of £10.80 per hour (as recommended by the platform based off of minimum wage rates) amounting to £3.60 for the approximate 20-minute runtime of the study [24]. The following demographic data was obtained from Prolific's database with self-reported information by the participants. The sample comprised 33% female participants and 67% male participants. They were 18-67 years old (M = 38 years). Thirty-six percent had a hybrid work arrangement where they sometimes worked from a central workplace and sometimes remotely, 32% always worked from a central place, 28% always worked remotely, and 4% indicated that their place of work changed regularly.

3.3.2 Term Selection. After reviewing the relevant literature, news articles, and laws and regulations, the lead researcher selected eight terms related to work monitoring to capture a diverse range of understanding of the subject. The term selection process was mainly inspired by the UK GDPR, as it is the primary legal framework governing this context, as well as the functionality and nature of work monitoring software and its practical applications. Adding a level of complexity to the selected terms, we chose to include terms with possible overlap in meanings (*monitoring*, *tracking*, *surveillance*) and varying degrees of prevalence and technicality (*remote work*, *consent*, *GDPR*, *keylogging*, *data minimisation*). For each term we developed a comprehensive baseline definition based on UK GDPR terminology and dictionary definitions, to ensure that they appropriately reflect the selected terms (see Table 1). Accuracy of participant definitions was assessed against the baseline definitions below. Each baseline definition was defined with the intention of capturing a wide range of participant understanding. If their definitions did not cover as many points from the definitions below, then their definitions would be deemed as less accurate. Below are the terms used as baseline for Study 1.

3.3.3 Survey design. The survey was hosted on LimeSurvey and consisted of three sections. The first part gauged the respondents' familiarity with each term through a 1-5 Likert scale (1="Never came across the term", 5="Very familiar with the term"). Next, on the following pages, participants were asked to provide their definitions for each term. The order of the terms was randomized. The survey questions are available in the Supplementary Materials. This study received favorable ethical opinion from the lead researcher's institutional School Research Ethics Committee.

3.3.4 Analysis. The analysis of our survey data involved quantitative and qualitative analyses.

Familiarity scores. Participants' familiarity scores were analysed through descriptive statistics. The median was used as a meaningful representation of central tendency, particularly because the familiarity Likert scale consisted of ordinal data.

Participant definition scores. To score their definitions, each baseline definition was broken down into smaller parts, which were used to help us score definitions provided by participants. This was done by sectioning parts of the baseline definition into substantive, clearly demarcated parts. Table 2 illustrates the coding and scoring process, using the Keylogging definition as an example. Each part of the definition received one point and was counted only once, even if it appeared multiple times in the same definition.

Each participant definition was rated independently by three researchers. Next, the scores were compiled and compared to identify any disagreements. Parts of the definition that had been given a score by two researchers were taken as endorsed by all three researchers. Those that received a score from only one researcher were discussed by the whole team and a collective decision was made on whether to keep or change the score. The data were analyzed using descriptive statistics, including mean, median, and standard deviation, to provide a comprehensive assessment of the results. Mean accuracy was calculated to account for the varying maximum scores across the eight terms, enabling a standardized comparison by expressing accuracy as a percentage of the total possible points.

As the data coding focused on parts of the definition (i.e., an item against which participant definitions were scored), the variation within definitions was obtained through a column analysis (see Appendix A) revealing the most used parts to define the terms. Combined with the thematic analysis, it indicated the depth of understanding from the definitions provided by participants.

Column analysis. A key aspect of this study was to examine the tendencies in participants' choice of words when defining the terms. We refer to appendix A for the insights derived from the column analysis. The column analyses show the percentage incidence of each part of the definition, reflecting how many participants included each component in their definitions. Seeking to understand how participants chose to interpret these terms, we analyzed them thematically [12]. During the scoring exercise, we took observational notes on each definition. These notes captured instances where we identified potential codes that could inform the subsequent thematic analysis. We then reviewed and discussed the notes added independently by each researcher, which led to the formation of three themes, namely expressivity, semantic precision, and conceptual framing. This approach allowed us to seamlessly integrate quantitative scoring with qualitative insights, ensuring that the themes were grounded in both the content and context of the participants' definitions. Tables 4 to 11 in Appendix A summarize the percentage incidence of all the definition parts which have informed our scoring process.

[1] It also meant we could meet practical constraints and stay within the allocated budget for the research.

Term	Researchers' Baseline Definitions	Resources
Monitoring	Monitoring is a general term that can encompass both tracking and surveillance, as well as other methods of collecting data about employees' work activities. Monitoring can be done through a variety of means, including software applications, network logs, and direct observation, and can serve a range of purposes, such as identifying inefficiencies or improving performance.	[59]
Keylogging	Keylogging is one of the types of monitoring software or hardware that records every keystroke made on a keyboard. It may be used by employers to track employee computer use, prevent unauthorised access to company systems, or investigate suspected security breaches or policy violations.	[60]
Tracking	Tracking in the context of work refers to the collection and analysis of data about an employee's work-related activities, such as the time spent on different tasks, or the websites they visited. This information can be used to monitor productivity and identify areas for improvement, but it might not necessarily involve the direct observation of an employee's work or communications.	[18]
Surveillance	Surveillance involves the direct observation of an employee's work or communications. This may include monitoring an employee's email or instant messages, listening in on phone conversations, or using video cameras to monitor the workplace. The goal of surveillance is typically to identify inappropriate or illegal behaviour, rather than simply monitoring productivity or performance.	[31]
Remote work	Remote work refers to a work arrangement where an employee is not physically present in a traditional office or workplace, but instead works from a remote location such as a home office, co-working space, or other remote location. This arrangement is made possible by technology such as video conferencing, remote desktop software, and other collaborative tools that allow employees to communicate and work together from different locations.	"[S]ituations where the work is fully or partly carried out on an alternative worksite other than the default place of work." [42]
GDPR	The GDPR (General Data Protection Regulation) is a comprehensive data privacy law that regulates the collection, processing, and storage of personal data for individuals located within the European Union (EU). The UK has retained the GDPR in its domestic law since Brexit. It therefore applies to all UK businesses that handle personal data, regardless of their size or industry sector.	"A part of European Union privacy law on the processing and storage of, and access to, personal data. Usually referred to as GDPR." [41]
Data minimisation	Data minimisation refers to the practice of limiting the collection, storage, and use of personal data to only what is necessary for a specific business purpose. This involves ensuring that only relevant and essential data is collected, and that it is not kept longer than necessary or used for purposes other than those for which it was collected.	As per Article 5 of the GDPR "1. Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)" [28]
Consent	In the context of work and personal data, consent refers to the voluntary and informed agreement given by an individual for their personal data to be collected, processed, and stored by a business for a specific purpose.	Voluntary agreement to a proposal, request, demand, etc.; acquiescence; an instance of this. Frequently in official or legal contexts: permission or approval for something.[58]. "Consent must be given freely, without duress or deception, and with sufficient legal competence to give it." [32]

Table 1: The Researchers' Baseline Definitions, with sources used in developing them.

Keylogging definition:' *'Keylogging is one of the types of monitoring software or hardware that records every keystroke made on a keyboard. It may be used by employers to track employee computer use, prevent unauthorised access to company systems, or investigate suspected security breaches or policy violations."*

	Parts of the definition					
Participant Definitions	Piece of software or Hardware.	Used to collect/ record/ track data.	Data processed are key presses on employee's keyboard.	Purpose is to track general computer use, as a measure of productivity.	Purpose is company security/ policy related.	Score
"where the computer records your keyboard activity"	1	1	1	0	0	3
"i am guessing its to do with logging of key information"	0	0	0	0	0	0

Table 2: Scoring participants' definition of Keylogging example

3.4 Quantitative Results

Familiarity scores. The purpose of the study 1 was to investigate the UK workers' familiarity towards and understanding of bossware terms. Aligning with the exploratory nature of this work, the analyses primarily relied on descriptive statistics to summarise and interpret the data. Hence, inferential statistical techniques were not relevant nor appropriate. The analysis of familiarity scores (see Table 3) indicated high ratings of familiarity for six terms out of eight, with the remaining two terms with lower familiarity scores being keylogging (*Mdn*= 3.00, i.e. Quite familiar with the term) and data minimisation (*Mdn*= 2.00, i.e. Came across the term but don't know much about it).

	Familiarity	Response Score				
	Median	Mean	Median	Highest possible score	Mean Accuracy (%)	*SD*
Monitoring	5.00	1.84	2.00	9	20	1.13
Keylogging	3.00	1.66	2.00	5	33	1.17
Tracking	4.00	0.87	1.00	6	15	0.88
Surveillance	5.00	1.65	1.00	13	13	1.02
Remote work	5.00	1.57	2.00	5	31	0.64
GDPR	5.00	1.78	1.00	7	25	1.55
Data minimisation	2.00	1.31	1.00	8	16	1.38
Consent	5.00	1.28	1.00	7	18	0.95

Table 3: Descriptive statistics

Participant definition scores. The definition scores were low for all terms, with mean scores ranging from 0.87 (Tracking) to 1.84 (Monitoring). Using the more standardized comparison of mean accuracy scores, the highest was for keylogging (33%) and the lowest for surveillance (13%).

Data minimisation and keylogging are technical terms. Their low familiarity median scores above indicate their low prevalence in participants' experiences. Mean accuracy for data minimisation was at 16% while it was higher for keylogging at 33%. This suggests that participants had better chances of inferring the meaning for keylogging rather than data minimisation. Keylogging actually had the highest mean accuracy score across the eight terms despite being the one of the less familiar terms for the participants. This indicates that a satisfactory understanding for the term was more easily inferred compared to the other seven terms.

GDPR was also a technical term, but participants rated themselves as very familiar with the term. They provided definitions with 25% mean accuracy, the third-highest mean accuracy score in this dataset. Familiarity scores were high for the five terms remaining to be reported. Listed in increasing levels of mean accuracy these were surveillance, tracking, consent, monitoring, and remote work. Those five terms were likely to be more prevalent than other technical terms and as expected scored high on familiarity ratings. As for surveillance, tracking, and monitoring, which are related terms in nature, there is a gradient in the levels of understanding of these terms evident from their differences in accuracy, with monitoring being the most accurate (20%), followed by tracking (15%), and surveillance (13%). The cause of this discrepancy could be either from the prevalence of these terms not being the same, or this may suggest a more fundamental problem in the discernment between those three terms. While participants were familiar with the concept of consent, they did not manage to provide satisfactory definitions which were specific to the topic of work monitoring, leading to an accuracy of 18%. Participants had better attempts at defining remote work, being a highly prevalent term, though their responses were at most 31% accurate on average. We should consider the above mean accuracy scores as participants' attempts at inferring meaning, and this was quite low (a maximum of 33%) across the eight terms.

Column analysis results. We now turn to column analysis results from the definition scoring process. The full tables are available in Appendix A and the most relevant parts to the discussion will be presented in this section.

Consent (See Table 4 in Appendix A) was predominantly defined by reference to 'agreement/approval' (44%) and 'permission' (37%). This covers a basic element of consent, but most definitions lacked specificity about the context of work.

Data minimisation (See Table 5 in Appendix A) tended to be mainly defined by making reference to 'mention[s] of limiting or reducing personal data' (36%), 'storage of personal data' (28%), and 'collection of personal data' (26%). Other parts of the legal concept of data minimisation was rarely covered by participants, e.g. 'used only for purposes it was collected for' (6%) and 'data [is] kept for no longer than necessary for purpose' (5%).

GDPR (See Table 6 in Appendix A) had nearly half participants (49%) correctly quote the longform format of the term. 31% of participants linked it to 'data privacy law' or 'concerns personal data'. Participants were less inclined to define the GDPR in terms of 'collection of data' (12%) or 'apply[ing] to organisations who handle personal data'(13%).

Keylogging (See Table 7 in Appendix A) had a high rate of participants choosing to define it with regards to 'used to collect/record/track data' (70%) and 'data processed are key presses on employee's keyboard' (66%). Only 21% made explicit mention of keylogging being achieved through a form of software or hardware. Few explained it in terms of its purpose, productivity-related (5%) or security-related (4%).

Remote work (See Table 8 in Appendix A) had most participants explaining it as working from an unspecified location away from their office (85%) and 66% defined it as a form of 'working from home'. No participants chose to explicitly explain it as working from a co-working space, and very few mentioned remote working as a 'work arrangement' (4%) and 'not being physically in-person at the office/workplace' (2%). 12% did mention remote working tools in their definitions.

Monitoring (See Table 9 in Appendix A) had 67% of participants defining it as a form of observation, though unspecified. 43% mention that the object of the monitoring is employee work activity in their definition, and 28% also gave a valid reason for the monitoring, e.g. productivity improvement. Only 21% mentioned 'digital observation' as part of their definition of monitoring. 19% defined the term making use of the words surveillance and/or tracking, essentially using them synonymously. Only 2% distinguished monitoring from surveillance or tracking when defining it. There were also very few choosing to define monitoring in terms of 'data', e.g. collecting data (14%), analysing data (4%), storing data (1%), processing data (0%).

Surveillance (See Table 10 in Appendix A) was defined by 57% of participants as a form of observation, though unspecified. Nearly half of participant, 41%, made use of the words monitoring and/or tracking, essentially using them synonymously to explain surveillance. 31% mentioned CCTV or video surveillance in their definition, while 17% mentioned 'digital observation' (through software). Few chose to mention a valid purpose for surveillance in their definitions: 'safety/security' (13%), 'compliance, investigating illegal or inappropriate behaviour' (9%), or 'productivity-related' (5%). Nearly no participants chose to explain surveillance with reference to 'data', e.g. 'collecting data' (9%), 'storing data' (3%), 'processing data' (1%), or 'analysing data' (1%). Only 1% distinguished surveillance from monitoring or tracking in their response.

Tracking (See Table 11 in Appendix A) was defined with a valid type of employee activity capable of being tracked by 38% of participants. 21% made mention of a valid reason for tracking employees e.g. productivity. 21% also used the terms monitoring and/or surveillance synonymously to explain tracking. No participant distinguished tracking from monitoring and/or surveillance. Mention of 'collecting data' (17%) and 'storing data' (10%) were more prevalent than 'analysing data' (1%), or 'processing data' (0%).

3.5 Thematic Analysis Results

Through the analysis, we identified three overarching themes from the definitions. The first theme noted the expression of uncertainty in participants' definitions as well as their associations of Surveillance and Keylogging as being more covert in nature. The second noted a lack of precision in how participants chose to define the terms, or the terms were especially precise (consent and remote work). Finally, there was a conceptual framing made evident when reading through some terms such as keylogging and GDPR which showed that participants chose to view some of the terms in more data-centric or person-centric lenses.

3.5.1 *Reluctance in expressing uncertainty and making associations with covertness.*

While some participants expressed their uncertainty when defining the terms, most, however, did not. Some simply admitted to not knowing and did not infer a meaning. The possibly more problematic group are those who did not express uncertainty and still gave a grossly inaccurate definition.

Extending this to an everyday context, many may hold inaccurate information or simply make wrong assumptions about what terms mean. Employees might not be vocal about what they understand, or they might hold a belief that their information is correct even if it is not. So it is important then to make this topic more approachable to employees so that they have a baseline of understanding that is rooted in viable information. It is to be noted that some terms such as 'data minimisation' had many incorrect definitions provided, which suggests that seemingly simple terms need to be operationalized and communicated to participants in research contexts and also explained clearly in work contexts.

We also observed that some participants associated some terms with being more covert or malicious, namely surveillance and keylogging. This highlights the potential for terminology such as these used in the context of work to evoke negative affect which may or may not be warranted depending on the purpose for the application of the relevant practice or technology. This negative association to monitoring terms could theoretically make employees more inclined to adopting counter-productive work behaviors.

> "Keylogging is the practice of covertly recording input signals into a computer from a keyboard for the computer not to be aware." - P29

> "Monitoring of an individual or group of individuals, usually covertly, using cameras, CCTV, police etc." – P35

P79 even defined it as a form of monitoring but "suspicious". P93 evokes the possible malicious aspect of keylogging when defining it:

> "Keylogging is where a 3rd party (often the IT department - but could also be a hacker) gets a record of every keystroke. This could be measures in keys per minute, or an actual transcript."

3.5.2 *Lack of precision in definitions.*

A lack of precision was also apparent when participants chose to use terms interchangeably to explain other terms, or used the term itself in many cases to define itself. The choice of expressing the definitions in this way points to the limited knowledge of the participants or lack of means to express distinctions between terms such as monitoring, surveillance, and tracking.

> "The use of surveillance in order to monitor employees behaviour, work, punctuality etc." – P26 on Monitoring

> "To monitor something over a period of time" – P54 on Tracking

Consent and remote work on the other hand showed quite high precision in terms of the definition being given being correct, but short and without context. This gives the impression of only one-dimensionality of their understanding. There was not much consideration for other possibilities of what the term could mean within their work situations.

> "simply put, agreement to something" – P45 on consent

> "To give permission" – P54 on consent

> "Working in a location other than the office" – P12 on remote work

P71 below gives a bit more context to their definition of remote work, mentioning the tools required for it.

> "Work you can do where you like, you normally only need a laptop and a internet connection" – P71 on remote work

3.5.3 *Impact of conceptual frames on definitions.*

We observed within the definitions for keylogging, tracking, and GDPR, that participants chose to define these terms with specific reference to 'data'. We labelled this as data-centric framing. For GDPR, it is within reasonable expectation that participants would guess that data might be part of the long-form definition. Keylogging, however, was thought of as a way of data being collected. Tracking was similar, with explicit mention of tasks being completed or not.

Contrastingly, participants chose to explain Monitoring and Surveillance in terms of the 'person,' we labelled this as person-centric framing. This repeatedly came through in the data as a person being observed or checking on a person.

It is important here to reconcile the two frames, as monitoring and surveillance also involve data being collected, while keylogging and tracking also include the person about which the data is being collected. These are important to make employees aware of in the digital age so that they may think critically about what can count as their personal data at work and whether they want it to be processed or not.

> "Some form of data logging that employees need to confirm to - maybe rules that need to be adhered to what entering data." – P10 on Keylogging
>
> "To watch something or someone closely - to watch how things change or someone's actions" – P55 on Monitoring
>
> "Watching over a person's activities" – P7 on Surveillance

3.6 Study 1 Discussion

This study highlights a discrepancy between employees' self-assessed familiarity with work monitoring terminology and their actual ability to provide accurate definitions. For example, while participants rated themselves as moderately familiar with terms such as keylogging (*Mdn* = 3.00) and very familiar with the 6 terms other than data minimisation, their definitions consistently lacked precision across the eight terms irrespective of their familiarity rating. The discrepancy suggests an overestimation of knowledge, potentially influenced by the Dunning-Kruger effect, where individuals with limited understanding tend to overestimate their competence [26]. This finding aligns with previous work in workplace information literacy, highlighting the challenge that employees face in understanding specialized terminology [49]. Should workers be more highly literate, it is conceivable that they would be able to recognize the nature, design, and purpose of technology being implemented in the workplace and evaluate it accordingly [56].

Going beyond knowledge accuracy scores, the data allowed us to understand in more depth how participants chose to define those eight terms. The qualitative element of this study allows for a nuanced understanding of employees' awareness of work monitoring practices. Participants often failed to express uncertainty, consider multiple interpretations of key terms, such as "consent" and "remote work", and frequently resorted to using terms, e.g. monitoring, to define themselves rather than making an effort to define them in other words and within the context of data in the workplace. The column analyses (See Appendix A) were also useful in giving more insight on the ways participants chose to or not to explain the terms. As expected from the overlapping terms (monitoring, surveillance, and tracking), there were many instances of one being explained by mention of the other as reflected in the thematic analysis as well. There were twice as many incidences of surveillance being explained in terms of monitoring and/or tracking compared to those two terms defined individually. This shows a particular overlap where surveillance may be construed as either monitoring or tracking but not necessarily the other way around. Surveillance, though, evoked associations of covertness in participants' understanding of it. This makes it distinct from monitoring and tracking.

Tracking was distinct from monitoring and surveillance as it was construed more through the lens of 'data' (being collected and stored) and also was explained primarily with a specific purpose or type of data being tracked as example. In contrast, monitoring and surveillance, as seen through the thematic analysis, was more related to observing the 'person' rather than the 'data'. As for remote work and consent, the word choice in explaining these terms align with the thematic analysis which found some one-dimensionality in the participants' definitions. The column analyses for these two terms corroborate this finding especially for remote work, while consent was more varied in the word choices, involving dimensions of 'giving by the individual' and relating to personal data. As for the three more technical terms (keylogging, GDPR, and data minimisation), keylogging was well understood by most of the participants. They made decent efforts to define GDPR and data minimisation as well. GDPR was more familiar to participants it seems as they managed to refer it to some of data processing. Data minimisation's definition was attempted to be inferred by participants, however, they did not cover the various points which would make it a complete definition as per the UK GDPR.

The lack of accuracy in awareness in addition to the overestimation of knowledge emphasizes a wider issue in workplace data-related education: employees are not equipped to critically engage with complex and evolving workplace monitoring practices. These insights expand the existing literature which has previously focused on broader aspects of literacy with regards to data protection. As a practical implication stemming from these findings, it is a call for reviewing the standards of workplace communication and training. The overestimation of knowledge, coupled with imprecise understanding, indicates a need for proactive dissemination of clear and accessible information about work monitoring practices and broader topics such as emerging technologies and the diverse categories of data-centric practices. Organizations should consider integrating targeted training programs or informational campaigns to address gaps in understanding across the organization, executives and employees alike. Additionally, HR policies should emphasize transparency in monitoring practices to foster a more informed workforce.

Despite the overestimation of knowledge with regards to work monitoring terminology, it is possible that workers can make valid inferences about how the law might protect them in this context. We turn to investigating the depth and limits of their legal awareness of the practice through interviews in the following study.

4 STUDY 2: INTERVIEWS

This study investigated UK employees' understanding of personal data protection in the context of workplace monitoring software. We sought to identify which types of electronic monitoring employees found acceptable or not, and their reasons for these views.

4.1 Methods

4.1.1 Participants and Recruitment. This exploratory study was conducted in August 2024 and received favourable ethical opinion from the lead researcher's institutional School Research Ethics

Committee. UK-based participants were recruited to ensure that participants had a similar experience regarding data protection and employment laws. An online expression of interest form generated on Microsoft Forms was shared on LinkedIn and on the lead researcher's University Microsoft Engage platform to call for participants. The criteria for eligibility required the participants to be over the age of 18, working in the UK, and speaking English. Participants who signed up were then sent an information sheet to review before proceeding with scheduling an interview and a consent form for signing. A Microsoft Forms link to a demographics form was also sent to the participant for them to complete prior to the interview.

Caine's work on local standards for sample sizes in research within the CHI community found that interviews conducted remotely had a mean sample size of 15 [15]. We decided on a target sample size of 20 to capture a range of perspectives and in-depth discussion. The compensation for participating in the study was a £10 Love2Shop voucher[2].

We recruited 20 participants but excluded one as they did not engage satisfactorily with the protocol. Among the participants, seven were female (37%), eleven were male (58%), and one participant (5%) preferred not to disclose this information. 68% of participants were aged between 25 and 34 years old, 21% were between the age of 35 and 44, and 11% were aged between 18 and 24. The participants self-reported their work industries as the following (in order of participant numbers 1-19): Professional services, Higher Education, Finance, Video Games, Marketing, Insurance, Data analytics and consultancy, Broadcasting, Sales, Pharmaceutical, Software development, Academic research, Finance, Financial services consulting, Gambling, Allied Healthcare (Assistant Psychologist), Public administration, Architecture, and Consulting Civil Engineer.

4.1.2 Design, Materials, and Procedure. Semi-structured interviews were conducted online through Microsoft Teams. The semi-structured format allowed for some flexibility in the questioning, enabling participants to express their thoughts more freely while ensuring the key topics were covered across all interviews. The transcription function in Microsoft Teams was used to generate transcripts. Interviews lasted approximately 45 minutes and participants received a financial incentive in the form of a £10 shopping voucher.

Consent was obtained before starting recordings and transcriptions. Participants were also reassured that their anonymity and confidentiality would be ensured prior to starting interviews. They were also reminded that there was no expectation of them having had experiences with work monitoring software, nor the laws and regulations around it, and were encouraged to freely share their thoughts on the topics presented.

The interview questions were structured in three main phases (see Supplementary Materials for the full interview guide). First, we established what the current knowledge and experience of the participants was regarding work monitoring software. We then assessed their knowledge of legal instruments that exist to protect their data. In the third phase, we presented participants with three fictional scenarios which included various work monitoring software functionalities inspired by what has been covered in the literature. Scenario one presented participants with a situation where keylogging and website and application monitoring was present on employee laptops. Scenario two presented them with a work monitoring software package being installed on employee computers including webcam monitoring and keylogging. The third scenario presented participants with a range of monitoring software including: keylogging, email monitoring, geolocation (GPS) tracking, webcam snapshots, and AI emotion recognition. Participants were asked a set of questions which was the same for the three scenarios. These questions asked for the purpose and necessity that the participant believed these functionalities were in place, the possible issues that are associated, and whether they believed these functionalities to be legal currently in the UK. Scenarios 1 and 3 had additional stages to them where an additional stage was added where a counter-productive measure was taken by the fictional employee. For example, Scenario 3 had an employee covering their camera to avoid being monitored, this was then followed with additional complications of the employee using a VPN to avoid being found out by the fictional employer while travelling overseas. Then with a final complication that the employer found out the employee's location through GPS. The associated questions for all of the additional complications revolved around the participants' opinion about the acts. They were also prompted to express whether they believed the act to be fair or not. Finally, they were also asked if the law should side with the employer or employee in those cases.

If time allowed in the interviews, we also had closing questions. These varied depending on the experience of the participants. Preset closing questions were drafted for those who had remote work experience, managerial experience, and finally more general questions. Respectively, some examples of these were if they believed that privacy while working in the office and privacy while working from home should be the same or not, if they used any dedicated tools or ways to monitor their team, and where they thought the lines should be drawn legally-speaking in relation to work monitoring software.

4.1.3 Analysis. We chose to use the reflexive thematic analysis (RTA) framework outlined by Braun and Clarke [12, 13] to analyze the interview data. We followed the six-step procedure as it is a widely recognized and respected method within qualitative research, ensuring this study's methodological rigor.

Transcripts were generated on Microsoft Teams and reviewed alongside the recording of each interview, except one instance where the participant preferred not having the conversation recorded; in their case, we used a file with interview notes as part of the analysis. The lead author read the transcripts several times. The first read through ensured that the transcript was free of personal information as part of the anonymization process, and also to correct any mistakes from the automatic transcription service. Potential codes were also noted as part of this read through. The codes were informed by our research question (deductive analysis), but we were also interested in identifying wider trends (inductive analysis). Initial codes were discussed with the rest of the research

[2] In Study 1 remuneration was handled through the Prolific platform. For Study 2 remuneration was handled by the researchers, and institutional policy forbids the use of cash. Effective rates of remuneration are very similar in both studies.

team. A second read-through was conducted, focusing on reviewing the identified codes and noting any new ones. Once all codes were obtained, the first author identified a set of themes that were revised and regularly discussed with the rest of the research team, which led to the formation of three key themes, which were further revised during work on this manuscript.

4.2 Study 2 Results

Three overarching themes were developed from the data: **Limited awareness of the law and work monitoring practices**, **Human-centered monitoring**, and **Issues of trust**. These themes will be discussed in more detail below.

4.2.1 Theme 1: Limited awareness of the law and work monitoring practices. This theme covers the key question this paper aimed to answer, what is the general state of employees' legal knowledge when it comes to work monitoring practices? We recognize that this theme was directly derived from the subject of the questions asked to participants.

Participants showed vague expressions of knowledge about the legal protections surrounding personal data and work monitoring practices. Some had no knowledge of the particular laws in place, rather they believed there was a law in place for it, e.g., P12: "I know there is law, but I don't remember the details." or P19: "I would suspect there's also some regulations in employment law, but I wouldn't know the details." Most did have some awareness that the UK GDPR was the most relevant legal framework here.

> "Yeah, I think a big one is the GDPR, yeah[...]. Uh, is it like a general general data protection? Right? I forgot exactly what it stands for, yeah." – P5

We note as well that the language being used above is tentative. It is understandable that the participants may have doubted their knowledge in the presence of a researcher who likely had the correct information, and so they might have felt the need to 'verify' their information using this tentative language. However, despite most participants having some idea that the GDPR was the key legal framework here, they could not provide a definition of it nor give specific details about how it protects personal data.

> "I'm pretty sure that GDPR, whatever it stands for, is one of the laws governing personal data and that's EU-wide legislation. I'm pretty sure that it applies in the UK." – P15

Even those who had received training about the GDPR in the past were not sure of the particulars of the regulations, although most participants recognized or guessed the presence of the Data Protection Act.

> "I know again there's GDPR, but I can't recall what it is off the top of my head, but we did have training for it and we do get reminded of it. But if I remember correctly just the Data Protection Act, and I believe that's what the NHS uses, it's like data, privacy, security law, but yeah." – P16

Participants were also not familiar with work monitoring practices. In general, they all referred to Microsoft Teams as being the way they keep in touch at work and that its status indicator would be the closest function to monitoring for productivity purposes. Some participants showed good awareness of what could possibly be tracked, though with some reservations about their certainty. Others had experienced bossware practices first-hand such as P9 who expressed that they had experience with their emails being monitored and accessed without their consent in the past. Also, P14 has a disclaimer on their laptops to say that all their activities can be monitored on the device. Below are some quotes of other participants, demonstrating their knowledge of work monitoring practices.

> "So what websites you've been on for, how much time, same for like which softwares you've used for how much time and uh yeah how much time off do you take, maybe frequency wise or how many hours are you officially online or like for how many of your working days?" – P6

> "I guess it could also range from like. You know, we're talking about online data, so like your history online history, the kind of thing, or even like less specific data. But I don't know, actually." – P5

> "Very high level understanding is that it is, you know, a piece of software that allows an employer to track activity online, but like laptop computer based activity of the of the employees." – P17

> "I think it's something that's preinstalled on your work laptop right? So, umm, it's something that's the IT department, could you know, just use it to hijack your work laptop and see what you're doing." – P12

Participants who had work roles in certain industries such as professional consulting services, finance, or healthcare were more attuned to the need for protection of client data, but they had not previously considered how those laws might apply to themselves as employees. It was interesting to note that employees, even though they consider the necessity for protection of client data, do not naturally think the same for their own data at their work.

> "interesting to think about this from an employee perspective because I think about it from a client perspective and what they have to do for their customers and clients." – P1

The low awareness and familiarity with the data protection laws and monitoring practices was evident, and so participants were provided definitions and examples where necessary to have them ready to consider the scenarios.

Participants' uncertainty about the law was clear when asked about whether they believed the functionalities mentioned in each scenario were legal in the UK or not. It is understandable here that they were more likely to use language or expressions which would make it so that they wanted to 'verify' their information. Nevertheless, it was interesting to note the strong emotions that came with the guesses participants made in this respect.

When asked whether they believed the functionalities mentioned to be legal, almost all participants were uncertain. P9, for example, believed that most of the functionalities were legal "because my previous company have it, so I think that it's already been approved and they are allowed to do it to a certain extent probably." Some ventured a guess and expressed their hope that it was not currently legal or to be made so.

> "I'm not sure because I don't know what the what is already in place, so I don't know if if I'm assuming. Obviously if there aren't concrete laws in policy and declaration and all that in place that companies feel like they can do whatever, especially with AI and stuff now."
>
> "I hope not. Yes, but I don't know." – P14

P8 and P10 expressed their views with a lot more certainty about the law. This was likely due to their experience with IT (P8), necessity of knowing the laws and regulations due to having had training on the matter, being in a highly confidential work environment, and having managerial duties (P10).

Participants were given the opportunity to describe their expectations of the law and how they would like the law to deal with workplace monitoring software. The following quotations show a range of what was discussed.

> "I mean, for an ideal world, I don't think there should be any monitoring except for security purposes, and that's only reason to be honest, to secure yourself and like company data or like feature property." – P9
>
> "There should be penalties basically for employers. If they are caught doing these things and they should have to disclose all the software that they have to use.– P11
>
> "And there needs to be guidelines towards the robustness of the software that's used [...] a threshold in terms of what kind of software is considered robust enough to protect both company-related data and personal data." – P13
>
> "My instinctive response would be I think the law should restrict employers from recording you, taking the pictures of you at work and effectively keeping the record of what you're typing at work." – P17

4.2.2 Theme 2: Human-centered monitoring and the dehumanizing power of technology. This theme was identified in the data as it captured a range of codes which were linked to the examples provided by participants on the communication with their managers being a key factor for productivity assessment, the necessity and accuracy (fit-for-purpose or not) of what was being monitored in scenarios, and how monitoring functionalities mentioned made them feel as employees.

Multiple participants expressed that an open line of communication with their employers to define and agree on what tasks or output to be completed in a particular timeframe was the best way of assessing productivity.

> "I mean, thankfully, productivity is measured in terms of outcome. So as long as that person is delivering or a place as some reasonable explanation, why not delivering us as much as I expected? Uh, I think there's no need to micro-observe what each of the employees is doing. I think that's unnecessary." – P3
>
> "I prefer to be measured to results and deadline." – P9
>
> "Maybe I am very conservative, but oh I would prefer supervisor conversations or having a chat with someone else rather than AI monitoring my face for example." – P1

We can also picture the lines of communication that exist within the employment context here. The implementation of bossware, in effect, subverts or negates completely the line of communication between employer and employee. When the manager goes from carbon-based to silicon-based, our actions also change. Counterproductive work behaviors were more likely to be endorsed by participants in situations where they believed the functionalities did not match the purpose of productivity assessment or security protocols. As P13 put it,

> "Relying on this kind of stuff, I think, and no communication in between with the employee. I think it's a detriment to workplace relationships."

P16 expressed the disgust felt if being monitored for extended periods of time, feeling dehumanized. P1 also made a point that AI should not be making diagnosing employees with depression as an example, and that this should be reserved for a human to do. Participants also expressed feelings of creepiness, fright, and weirdness when considering monitoring software being applied, especially for scenarios involving camera monitoring.

Participants interestingly noted how some types of bossware may act even as an ally of sorts and help them at work beyond being useful for security or health and safety purposes. Referring to the lines of communication that exist in the work context as mentioned above, rather than employer-employee, there can also be lines of communication open to other colleagues through software, as was the case for P16, which allows them to check in with each other and so in a way using a 'low-intrusiveness' monitoring software such as MS Teams allows them to look after each other. P16 mentioned an instance where a colleague was caught in a car accident and colleagues managed to find out that something wrong had happened based off of the colleague's Teams status having been offline for longer than expected. A similar argument was made by P9, who believed that GPS tracking was a useful feature to have on their company phones to give employees some sense of safety while doing site visits.

P18 also believed in the potential benefit of having AI functionality applied in the work context to ensure colleagues were satisfied at work, as a human may not pick up on signs that they are not doing well. This is counter to what most participants believed, however. The general attitude towards AI in the other interviews all expressed the feeling that using AI in the monitoring context was a step too far. P13 shared a contrary view to this:

> "AI analytics is at the end of the day it's just an intelligent software. I think it could provide the wrong kind of outcome [...] when the manager kind of leans into it to see what the results of those analytics are then... Maybe it's a cheaper way for managers to monitor employees, but I would say it could lead to the wrong results." – P13

Similarly, P2 mentions how bossware might lead to wrong conclusions about employee performance:

> "I think like with anything that is reliant on data, the number alone doesn't tell you the story because it doesn't tell you actually the person wasn't clicking anything because they're a lawyer and they spent, you know, an hour reading case law, which is a valid use of their time." – P2

4.2.3 Theme 3: Issues of trust between the employee and their employer, technology, and the law. This theme relates to participants' trust in their employer, in legislation to protect them at work, and in the technology itself.

Many participants mentioned the lack of trust between employees and their employers as a result of the implementation of bossware. This could either be a signal of a lack of trust the employer has towards their employees prompting the application of bossware, or that it was applied after the trust between the two parties was eroded and so required bossware to be applied. Transparency of monitoring being applied was called for by most participants. Some even were accepting of the fact of being monitored should their employer make it clear as to why and how they were being monitored.

> "If it's that important to the company, then that means I think there is just the lack of trust and I don't really... I wouldn't want to work for a company that doesn't trust that I do my job properly, and I also think there are many ways where it will be found out that I don't do my job properly and it doesn't have to involve them seeing my face or then, you know, having any software, keylogging, whatever." – P1

> "[As] an analogy, I wouldn't want my parents to be checking my what websites I monitor or what I go into even growing up as a child, so if I could extend it to the workplace." – P13

> "I think that between employer and employee that there has to be a level of trust in that relationship, for it to be beneficial for both parties. I think that kind of software would erode that trust, which may be detrimental to both parties." – P19

Participants' also expressed trust or hopefulness towards the law being designed to protect them.

> "I agree there should be a law in place that protects mistreatment from having these kind of policies in place, even though I'm not sure whether the UK law would even allow for these policies to be there to begin with." – P13

> "My instinctive response would be I think the law should restrict employers from recording you, taking the pictures of you at work and effectively keeping the record of what you're typing at work." – P17

Despite recognizing the hope that the law might protect them, P16 points out:

> "So personally I would hope that the law stands with someone who says I do not consent to this because I think that's a very important, but realistically, and knowing how the world works, they're probably gonna side with the employer." – P16

Participants, showing some distrust in technology, found the bossware webcam functionality and the implementation of AI within it problematic. They could not trust that the system will not have some form of bias making it unfair on workers to be monitored in such a way.

> "Uh, the issue is that given that there is a sort of black box behind how it processes the information and how it speaks out our results, how would you trust? Are we just going to trust this to be accurate and reliable?" – P3

> "AI's are a very problematic area right now. It's not necessarily in a state where it's reliable, but people again are very keen on developing yet and turn a blind eye or are ignorant sort of the potential dangers to AI and using AI driven data. " – P4

Some, however, believed that the AI function mentioned in the third scenario could be used for positive reasons in the workplace which can benefit the employees and company in general.

> "[employer might use this for] optimizing workflow but doing it in a way where. It's very much data driven rather than some human needing to take time out of their day to monitor, to analyze the data itself. They can just get a sentence from [the AI] about who's doing all this automatically. Uh cut down on the operational times of that part of the HR input." – P4

> "I would think that if they were informed that they were going to use these measures, I don't see it in a in a bad way, because sometimes people struggle to express how they feel, or sometimes they feel like they don't have the right people to talk to when they feel frustrated about a project or a task. Or they maybe they feel unfulfilled, etcetera. So in this case, I would say that this could help. That could be very helpful for the employer and HR and all the right people that deal with this in a company to, let's say, to relink a bit to this human side of things." – P18

4.3 Study 2 Discussion

This study aimed to evaluate employees' legal awareness regarding work monitoring software practices, revealing a gap in their understanding. Although some participants had received GDPR training at work, remembering the specifics was a tall order for most, with only a few exceptions among participants whose work roles provided direct exposure to the topic. This finding points to the weakness of data protection training sessions. Some had more experience with the topic because of their line of work, and so had clear ideas on what they could expect from the law with a certain level of certainty. Most participants, however, demonstrated uncertainty towards what was likely to be legal and what was not. Fictional scenarios involving AI implementations elicited more concern, perhaps due to the novelty and ethical ambiguity of such technologies. Interestingly, some participants believed certain functionalities might be legally permissible simply because laws and regulations had not yet addressed those contexts, highlighting potential gray areas in the law.

These findings further our understanding of UK employees' legal awareness in the workplace. It is evident from the data that there is a disconnect between the law and employees' comprehension of it within the context of this study. While previous research has been quite compartmentalized in its approach, assessing employee psychological attitudes towards work monitoring or legal breakdowns of how the law applies with regards to bossware, this study puts forward an approach which focuses on the experience of the employee at the center of the monitored workplace. We have uncovered their uncertainties and assumptions about the law in this regard.

There are practical implications for workplace training and policy design that we can take away from this study. GDPR training sessions as they are currently taught may be insufficient in promoting lasting understanding among employees, and so may benefit from a review to better engage employees. For example, training programs which tie together legal principles to common workplace practices could enhance retention and practical application of data protection principles. Additionally, organizations should consider more transparent communication about monitoring practices and their legal basis to build employee trust and awareness, this may also make it more of a common discussion point which would benefit this 'data literacy'.

5 GENERAL DISCUSSION

This research set out to explore employees' comprehension of work monitoring terminology and their awareness of legal protections regarding bossware. Study 1 examined the familiarity and actual knowledge of 100 UK employees through an online survey, and Study 2 assessed the legal awareness of 19 UK employees regarding work monitoring software through online interviews. The findings revealed that employees were not accurate in providing definitions for eight terms linked to work monitoring, they also rated themselves highly on familiarity with those terms prior to defining them. Moreover, thematic analysis in Study 1 revealed that participants found it challenging to distinguish between terms which are similar in nature (e.g. monitoring and surveillance). Participants either were unaware of gaps in their knowledge (not knowing what they did not know) or did not express uncertainty when defining the terms, instead proceeding to provide incomplete or imprecise definitions. Through Study 2 we found that employees were not aware of their legal protections in the workplace regarding monitoring. Even those who had experience with the GDPR showed uncertainty in their answers to whether particular functionalities were legal in the UK. Furthermore, they mentioned interesting avenues for the law to better protect their rights. One of these suggestions was to look into the robustness of monitoring software while another was for limits to be set to prevent monitoring their faces or emotions. Together, these results contribute to our understanding of the state of employees' comprehension of work monitoring terminology and their awareness of legal issues surrounding workplace monitoring.

While Study 1 had no direct precedent in the literature, Study 2 corroborated previous work while providing a novel contribution regarding employee legal awareness. For example, supporting findings by Jeske [43], P16 commented on the benefit of using the Microsoft Teams status bar and a WhatsApp channel with all colleagues to keep an eye out for each other. This was especially important to them in situations of doing site visits. Another aspect which has been referred to in previous work is the dehumanization of employees, which follows the elimination of interaction between employer and employee and replaces it with a one-way system between the employee and the monitoring software [4]. This means that the issues linked with having employees monitored electronically as reported over twenty years ago are still valid today. The situation is worse now, given the array of functionalities modern bossware can leverage. For example, the video monitoring through webcams was unsettling for a few participants in Study 2, and the mention of AI emotion assessment through webcams made them even more frustrated at the capabilities of bossware. This reflects previous work by Roemmich et al. [68] which found that employees in the United States perceived emotion AI to deeply violate their privacy which can translate in worsened working experiences (organizational trust and job satisfaction) for employees. The functionalities of new technologies applied to the bossware context may likely accentuate prior findings in the literature. It would therefore be useful for researchers to review employees' perceptions of new bossware practices, as these may have evolved just as the technology has. A potential area for reform would be the review of GDPR training best practices to better inform employees about personal data protection and their rights at work. Therefore, legislators and policymakers should regularly revise the legal landscape to keep up with evolving technology and prioritize employees' rights above company productivity metrics.

5.1 Implications for Research, Law, and Policy

The key implication which these studies highlight is that no one engaged in this issue —researchers, worker representatives, employers, legislators or policymakers— should take for granted that workers have accurate working definitions of these terms nor do they have sufficient knowledge of the limits of legality on monitoring practices. It is imperative to find a solution to this gap in employees' knowledge: should bossware be applied in workplaces, the negative effects such as worsening performance at work are likely to surface [45]. Furthermore, we believe that without worker awareness of the technical and legal context of their employers' monitoring practices, resistance to workplace monitoring would not be a natural inclination for employees, leading to their rights being breached.

5.2 Limitations and Future work

In Study 1, we intentionally limited the terminology list to eight terms to ensure that the data remained manageable within the scope of our research resources. We chose these a priori on the basis of their significance and relevance to the topic. The diversity in the selection of the eight terms for this study was done in such a way as to highlight possible conflation of terms such as monitoring, surveillance, and tracking, and the ability of workers to make valid inferences for specialised terms such as data minimisation. Although we remain satisfied that the choices were appropriate, by restricting the number of terms we asked participants define, we constrained the expression of their knowledge on the matter. They may have had stronger knowledge on other related terms, for example. The paucity of knowledge of the eight terms suggests this is unlikely, but we cannot rule it out. For future work, it would be beneficial to determine, perhaps by running focus groups, that there are no parallel collections of terms that are in use and that people clearly understand. (This seems unlikely given the findings of Study 2, but it would still be work excluding the possibility.) As for the limitations arising from our sample, the 100 workers were recruited through Prolific and so might capture a type of worker which could share some level of similarity in their work patterns hence limiting the diversity and generalizability of the sample. Future research, as well as finding other avenues for recruiting a diverse sample, should explore other methods of assessing familiarity, understanding, and inference of meaning by employees across different work roles, industries, or jurisdictions. This could serve to examine which factors influence employee comprehension of work monitoring practices and other data-centric practices.

As for Study 2, while it is good that the participants were drawn from a variety of industries, several had experience with the GDPR due to their work roles or company-provided training involving the GDPR. It is reasonable to assume that this gave these participants more knowledge of work monitoring practices than the 'median' worker. Nevertheless, we believe this further strengthens the point that even those with prior knowledge were still unsure of what to expect in terms of legality for monitoring practices. The generalization of findings may be limited to the UK and the participants' work industries. Future research should further investigate legal awareness by comparing GDPR and data protection training policies across companies. We would also recommend broadening the sample to other EU countries as they also use the GDPR, as well as comparative work in jurisdictions that do not have GDPR-like legislation. There is also an opportunity for future work to approach non-office type workers such as warehouse or gig workers on their understanding of work monitoring practices and its legality. For many of them, work monitoring may be a prerequisite to being able to undertake such work.

6 CONCLUSION

This paper presented two studies which investigate employees' awareness of work monitoring terminology and their awareness of the legal context surrounding work monitoring. Through Study 1, we found that employees overestimated their knowledge on the topic as they rated themselves as familiar with key terms and yet scored poorly on accuracy compared with technically complete definitions when asked to define them. Study 2 showed that employees do not have sufficient knowledge of work monitoring, both as a practice and the nuances of its legality. Both of these studies highlight a possible lack of transparency about or inaccessibility to information which might be too complex for the average person to comprehend. We contribute to the research on work monitoring by establishing a baseline of expectation of employees' knowledge on the topic. This is important for academics beyond HCI conducting research in this area as they will have to properly inform their participants of the practice or its legality where relevant. Without priming participants with accurate information, inaccuracies may occur in the data collected as a result of assumptions and misunderstandings. These findings are crucial in practical contexts, as without proper awareness of these matters, employees may not recognize potential issues with their data being processed for monitoring purposes at work, nor would they know what they can do to challenge such practices. Developing a shared understanding of work monitoring practices should be an immediate priority for stakeholders involved to safeguard employee rights.

REFERENCES

[1] M. Addis and M. Kutar. 2018. The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. In *UK Academy for Information Systems Conference Proceedings 2018*, Vol. 29. UK Academy for Information Systems, Newcastle-upon-Tyne, UK.

[2] J. R. Aiello and K. J. Kolb. 1995. Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress. *Journal of Applied Psychology* 80, 3 (1995), 339–353. https://doi.org/10.1037/0021-9010.80.3.339

[3] I. Ajunwa, K. Crawford, and J. Schultz. 2017. Limitless Worker Surveillance. *California Law Review* 105 (2017), 735–776. https://doi.org/10.15779/Z38BR8MF94

[4] G. S. Alder. 1998. Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives. *Journal of Business Ethics* 17, 7 (May 1998), 729–743. https://doi.org/10.1023/A:1005776615072

[5] G. S. Alder and P. K. Tompkins. 1997. Electronic Performance Monitoring: An Organizational Justice and Concertive Control Perspective. *Management Communication Quarterly* 10, 3 (Feb. 1997), 259–288. https://doi.org/10.1177/0893318997010003001

[6] A. Aloisi and V. De Stefano. 2022. Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon. *International Labour Review* 161, 2 (2022), 289–314. https://doi.org/10.1111/ilr.12219

[7] K. Ball. 2010. Workplace Surveillance: An Overview. *Labor History* 51, 1 (Feb. 2010), 87–106. https://doi.org/10.1080/00236561003654776

[8] K. Ball. 2022. Surveillance in the Workplace: Past, Present, and Future. *Surveillance & Society* 20, 4 (Dec. 2022), 455–461. https://doi.org/10.24908/ss.v20i4.15805

[9] R. Ballard. 2022. Everyday Resistance: Theorising How the 'Weak' Change the World. In *The Routledge Handbook of Social Change*, Richard Ballard and Clive Barnett (Eds.). Routledge, London, 400.

[10] L. K. Bartels and C. R. Nordstrom. 2012. Examining Big Brother's Purpose for Using Electronic Performance Monitoring. *Performance Improvement Quarterly* 25, 2 (Jan. 2012), 65–77. https://doi.org/10.1002/piq.20140

[11] D. P. Bhave. 2014. The Invisible Eye? Electronic Performance Monitoring and Employee Job Performance. *Personnel Psychology* 67, 3 (2014), 605–635. https://doi.org/10.1111/peps.12046

[12] V. Braun and V. Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[13] V. Braun and V. Clarke. 2019. Reflecting on Reflexive Thematic Analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (Aug. 2019), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

[14] N. Brewer. 1995. The Effects of Monitoring Individual and Group Performance on the Distribution of Effort Across Tasks1. *Journal of Applied Social Psychology* 25, 9 (1995), 760–777. https://doi.org/10.1111/j.1559-1816.1995.tb01774.x

[15] K. Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 981–992. https://doi.org/10.1145/2858036.2858498

[16] M. Cantor. 2023. Idle No More: How Automatic Mouse Jigglers Are Taking on Nosy Bosses. *The Guardian* (March 2023).

[17] J. Chalykoff and T. A. Kochan. 1989. Computer-Aided Monitoring: Its Influence on Employee Job Satisfaction and Turnover. *Personnel Psychology* 42, 4 (Dec. 1989), 807–834. https://doi.org/10.1111/j.1744-6570.1989.tb00676.x

[18] D. Chandler and R. Munday. 2016. Tracking. In *A Dictionary of Social Media*. Oxford University Press, Oxford, UK.

[19] P. Collins. 2024. Managing Technology That Manages People: Regulatory Strategies for the UK. https://doi.org/10.2139/ssrn.4987711 social science research network:4987711

[20] P. Collins and S. Marassi. 2021. Is That Lawful? Data Privacy, Monitoring and Fitness Trackers in the Workplace. *InternationalJournalofComparativeLabourLaw* 37(1) (2021), 65–94.

[21] T. U. Congress. 2018. I'll Be Watching You - What Is Workplace Monitoring? | TUC.

[22] T. U. Congress. 2020. Technology Managing People | TUC.

[23] B. Cyphers and K. Gullo. 2020. Inside the Invasive, Secretive “Bossware” Tracking Workers.

[24] G. Denison. 2023. How Much Should You Pay Research Participants?

[25] R. Derousseau. 2017. The Tech That Tracks Your Movements at Work.

[26] D. Dunning. 2011. Chapter Five - The Dunning–Kruger Effect: On Being Ignorant of One's Own Ignorance. In *Advances in Experimental Social Psychology*, James M. Olson and Mark P. Zanna (Eds.). Vol. 44. Academic Press, Cambridge, MA, USA, 247–296. https://doi.org/10.1016/B978-0-12-385522-0.00005-6

[27] ECHR. 1953. European Convention on Human Rights.

[28] European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council.

[29] G. Gaudio. 2021. Algorithmic Bosses Can't Lie! How to Foster Transparency and Limit Abuses of the New Algorithmic Managers. *Comparative Labor Law & Policy Journal* 42, 3 (2021), 707–742.

[30] GDPR.EU. 2019. *GDPR Small Business Survey.* Technical Report. GDPR.EU.

[31] G. Gooch and M. Williams. 2007. Surveillance. In *A Dictionary of Law Enforcement.* Oxford University Press, Oxford, UK.

[32] G. Gooch and M. Williams. 2015. Consent. In *A Dictionary of Law Enforcement.* Oxford University Press, Oxford, UK.

[33] S. J. J. Gould. 2024. Stochastic Machine Witnesses at Work: Today's Critiques of Taylorism Are Inadequate for Workplace Surveillance Epistemologies of the Future. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3613904.3642206

[34] M. Hickok and N. Maslej. 2023. A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools. *AI and Ethics* 3, 3 (Aug. 2023), 673–687. https://doi.org/10.1007/s43681-023-00275-8

[35] P. J. Holland, B. Cooper, and R. Hecker. 2015. Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type. *Personnel Review* 44, 1 (Jan. 2015), 161–175. https://doi.org/10.1108/PR-11-2013-0211

[36] ICO. 2011. *The Employment Practices Code.* Technical Report. ICO.

[37] ICO. 2022. Employment Practices: Monitoring at Work Draft Guidance.

[38] ICO. 2024. Data Protection and Monitoring Workers.

[39] ICO. 2024. Penalties.

[40] ICO. 2024. The UK GDPR.

[41] D. Ince. 2019. General Data Protection Regulation. In *A Dictionary of the Internet.* Oxford University Press, Oxford, UK.

[42] International Labour Organization. 2020. *Defining and Measuring Remote Work, Telework, Work at Home and Home-Based Work.* ILO Technical Note. International Labour Organization.

[43] D. Jeske. 2021. Monitoring Remote Employees: Implications for HR. *Strategic HR Review* 20, 2 (July 2021), 42–46. https://doi.org/10.1108/SHR-10-2020-0089

[44] D. Jeske. 2022. Remote Workers' Experiences with Electronic Monitoring during Covid-19: Implications and Recommendations. *International Journal of Workplace Health Management* 15, 3 (Jan. 2022), 393–409. https://doi.org/10.1108/IJWHM-02-2021-0042

[45] D. Jeske and A. M. Santuzzi. 2015. Monitoring What and How: Psychological Implications of Electronic Performance Monitoring. *New Technology, Work and Employment* 30, 1 (2015), 62–78. https://doi.org/10.1111/ntwe.12039

[46] T. Kalischko and R. Riedl. 2021. Electronic Performance Monitoring in the Digital Workplace: Conceptualization, Review of Effects and Moderators, and Future Research Opportunities. *Frontiers in Psychology* 12 (May 2021). https://doi.org/10.3389/fpsyg.2021.633031

[47] J. Kelly. 2020. Big British Bank Barclays Accused Of Spying On Employees—This May Be The New Trend.

[48] G. Lockwood and V. Nath. 2020. The Monitoring of Tele-Homeworkers in the UK: Legal and Managerial Implications. *International Journal of Law and Management* 63, 4 (Jan. 2020), 396–416. https://doi.org/10.1108/IJLMA-10-2020-0281

[49] K. Mahmood. 2016. Do People Overestimate Their Information Literacy Skills? A Systematic Review of Empirical Evidence on the Dunning-Kruger Effect. *Communications in Information Literacy* 10, 2 (Dec. 2016), 199–213. https://doi.org/10.15760/comminfolit.2016.10.2.24

[50] K. Makortoff. 2020. Barclays Using 'Big Brother' Tactics to Spy on Staff, Says TUC. *The Guardian* (Feb. 2020).

[51] A. J. Martin, J. M. Wellen, and M. R. Grimmer. 2016. An Eye on Your Work: How Empowerment Affects the Relationship between Electronic Surveillance and Counterproductive Work Behaviours. *The International Journal of Human Resource Management* 27, 21 (Nov. 2016), 2635–2651. https://doi.org/10.1080/09585192.2016.1225313

[52] K. Martin and R. E. Freeman. 2003. Some Problems with Employee Monitoring. *Journal of Business Ethics* 43, 4 (April 2003), 353–361. https://doi.org/10.1023/A:1023014112461

[53] W. Martinez, J. Benerradi, S. Midha, H. A. Maior, and M. L. Wilson. 2022. Understanding the Ethical Concerns for Neurotechnology in the Future of Work. In *Proceedings of the 1st Annual Meeting of the Symposium on Human-Computer Interaction for Work (CHIWORK '22)*. Association for Computing Machinery, New York, NY, USA, 1–19. https://doi.org/10.1145/3533406.3533423

[54] C. McParland and R. Connolly. 2019. Employee Monitoring in the Digital Era: Managing the Impact of Innovation. https://doi.org/10.2139/ssrn.3492245 social science research network:3492245

[55] D. M. Nebeker and B. C. Tatum. 1993. The Effects of Computer Monitoring, Standards, and Rewards on Work Performance, Job Satisfaction, and Stress1. *Journal of Applied Social Psychology* 23, 7 (April 1993), 508–536. https://doi.org/10.1111/j.1559-1816.1993.tb01101.x

[56] S. Nikou, M. D. Reuver, and M. M. Kanafi. 2022. Workplace Literacy Skills—How Information and Digital Literacy Affect Adoption of Digital Technology. *Journal of Documentation* 78, 7 (May 2022), 371–391. https://doi.org/10.1108/JD-12-2021-0241

[57] M. Otto. 2015. The Right to Privacy in Employment: In Search of the European Model of Protection. *European Labour Law Journal* 6, 4 (Dec. 2015), 343–363. https://doi.org/10.1177/201395251500600404

[58] Oxford English Dictionary. 2023. Consent, n.

[59] Oxford English Dictionary. 2023. Monitor, v.

[60] Oxford English Dictionary. 2024. Keylogging, n.

[61] Parliament of the United Kingdom. 1996. Employment Rights Act 1996.

[62] Parliament of the United Kingdom. 1998. Human Rights Act.

[63] Parliament of the United Kingdom. 2018. Data Protection Act. , 379 pages.

[64] L. E. Pleger, K. Guirguis, and A. Mertes. 2021. Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security. *Computers in Human Behavior* 122 (Sept. 2021), 106830. https://doi.org/10.1016/j.chb.2021.106830

[65] B. Quinn and J. Jackson. 2016. Daily Telegraph to Withdraw Devices Monitoring Time at Desk after Criticism. *The Guardian* (Jan. 2016).

[66] D. M. Ravid, D. L. Tomczak, J. C. White, and T. S. Behrend. 2020. EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management* 46, 1 (Jan. 2020), 100–126. https://doi.org/10.1177/0149206319869435

[67] D. M. Ravid, J. C. White, D. L. Tomczak, A. F. Miles, and T. S. Behrend. 2023. A Meta-Analysis of the Effects of Electronic Performance Monitoring on Work Outcomes. *Personnel Psychology* 76, 1 (2023), 5–40. https://doi.org/10.1111/peps.12514

[68] K. Roemmich, F. Schaub, and N. Andalibi. 2023. Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3544548.3580950

[69] S. Sannon, B. Sun, and D. Cosley. 2022. Privacy, Surveillance, and Power in the Gig Economy. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3491102.3502083

[70] G. Sewell and J. R. Barker. 2006. Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance. *Academy of Management Review* 31, 4 (Oct. 2006), 934–961. https://doi.org/10.5465/amr.2006.22527466

[71] S. Sirur, J. R. Nurse, and H. Webb. 2018. Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18)*. Association for Computing Machinery, New York, NY, USA, 88–95. https://doi.org/10.1145/3267357.3267368

[72] J. M. Stanton and E. M. Weiss. 2000. Electronic Monitoring in Their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance. *Computers in Human Behavior* 16, 4 (July 2000), 423–440. https://doi.org/10.1016/S0747-5632(00)00018-2

[73] L. Stark, A. Stanhaus, and D. L. Anthony. 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 (Sept. 2020), 1074–1088. https://doi.org/10.1002/asi.24342

[74] S. Taneja, M. G. Pryor, and L. A. Toombs. 2011. Frederick W. Taylor's Scientific Management Principles: Relevance and Validity. *Journal of Applied Management and Entrepreneurship* 16, 3 (July 2011), 60–78.

[75] F. W. Taylor. 1911. *The Principles of Scientific Management.* Harper & Brothers, New York, NY, USA and London, UK.

[76] D. L. Tomczak, T. S. Behrend, J. Willford, and W. P. Jimenez. 2020. “I Didn't Agree to These Terms”: Electronic Performance Monitoring Violates the Psychological Contract. https://doi.org/10.31234/osf.io/qax9u

[77] D. L. Wells, R. H. Moorman, and J. M. Werner. 2007. The Impact of the Perceived Purpose of Electronic Performance Monitoring on an Array of Attitudinal Variables. *Human Resource Development Quarterly* 18, 1 (2007), 121–138. https://doi.org/10.1002/hrdq.1194

[78] R. B. Zajonc. 1965. Social Facilitation. *Science* 149, 3681 (July 1965), 269–274. https://doi.org/10.1126/science.149.3681.269

A DEFINITION SCORING COLUMN ANALYSIS TABLES

Definition	Parts of the definition	% incidence
‘‘In the context of work and personal data, consent refers to the voluntary and informed agreement given by an individual for their personal data to be collected, processed, and stored by a business for a specific purpose.”	Agreement/Approval	44
	Permission	37
	Given by the individual	18
	Personal Data	14
	Collected, processed, and stored by a business for a specific purpose	8
	Informed	5
	Voluntary	2

Table 4: Consent column analysis

Definition	Parts of the definition	% incidence
“Data minimisation refers to the practice of limiting the collection, storage, and use of personal data to only what is necessary for a specific business purpose. This involves ensuring that only relevant and essential data is collected, and that it is not kept longer than necessary or used for purposes other than those for which it was collected.”	Mentions limiting or reducing personal data	36
	Storage of personal data	28
	Collection of personal data	26
	Data collected is essential/necessary to achieve purpose	16
	Only relevant data is collected	9
	Used only for purposes it was collected for	6
	Use of personal data	5
	Data is kept no longer than necessary for purpose	5

Table 5: Data minimisation column analysis

Definition	Parts of the definition	% incidence
“The GDPR (General Data Protection Regulation) is a comprehensive data privacy law that regulates the collection, processing, and storage of personal data for individuals located within the European Union (EU). The UK has retained the GDPR in its domestic law since Brexit. It therefore applies to all UK businesses that handle personal data, regardless of their size or industry sector.”	Correct term longform- General Data Protection Regulations (accept omitting General)	49
	Data privacy law	31
	Concerns personal data: Data which can be used to identify a person is regarded as personal data	31
	Processing of data	21
	Storage of data	21
	Collection of data	12
	Applies to organisations who handle personal data	13

Table 6: GDPR column analysis

Definition	Parts of the definition	% incidence
“Keylogging is one of the types of monitoring software or hardware that records every keystroke made on a keyboard. It may be used by employers to track employee computer use, prevent unauthorised access to company systems, or investigate suspected security breaches or policy violations.”	Used to collect/record/track data	70
	Data processed are key presses on employee’s keyboard	66
	Piece of software or Hardware	21
	Purpose is to track general computer use, as a measure of productivity	5
	Purpose is company security/policy related.	4

Table 7: Keylogging column analysis

Definition	Parts of the definition	% incidence
"Remote work refers to a work arrangement where an employee is not physically present in a traditional office or workplace, but instead works from a remote location such as a home office, co-working space, or other remote location. This arrangement is made possible by technology such as video conferencing, remote desktop software, and other collaborative tools that allow employees to communicate and work together from different locations."	Working from unspecified remote location away from office	85
	Working from home	66
	Remote work tools: video conferencing software, remote desktop	12
	Work arrangement	4
	Not physically present in-person at office/workplace	2
	Working from co-working space	0

Table 8: Remote work column analysis

Definition	Parts of the definition	% incidence
"Monitoring is a general term that can encompass both tracking and surveillance, as well as other methods of collecting data about employees' work activities. Monitoring can be done through a variety of means, including software applications, network logs, and direct observation, and can serve a range of purposes, such as identifying inefficiencies or improving performance."	Observation (unspecified)	67
	Data processed is about employee work activity	43
	A valid reason for monitoring employees (e.g. productivity improvement)	28
	Digital observation	21
	Synonymous with Tracking and/or Surveillance	19
	Collecting data	14
	Physical observation	6
	Analysing Data	4
	Distinguishing from tracking and/or surveillance	2
	Storing data	1
	Processing data	0

Table 9: Monitoring column analysis

Definition	Parts of the definition	% incidence
"Surveillance involves the direct observation of an employee's work or communications. This may include monitoring an employee's email or instant messages, listening in on phone conversations, or using video cameras to monitor the workplace. The goal of surveillance is typically to identify inappropriate or illegal behaviour, rather than simply monitoring productivity or performance."	Observation (unspecified)	57
	Synonymous with Monitoring and/or Tracking	41
	CCTV/ Video surveillance	31
	Data processed is about employee work activity	18
	Digital observation (through software)	17
	Valid purpose - Safety/Security	13
	Collecting Data	9
	Valid purpose – compliance, investigating illegal or inappropriate behaviour	9
	Valid purpose – productivity related	5
	Storing Data	3
	Processing Data	1
	Analysing Data	1
	In-person observation of employee	1
	Distinguishing from Monitoring and/or Tracking	1
	Data processed is about employee communications	0

Table 10: Surveillance column analysis

Definition	**Parts of the definition**	**% incidence**
"Tracking in the context of work refers to the collection and analysis of data about an employee's work-related activities, such as the time spent on different tasks, or the websites they visited. This information can be used to monitor productivity and identify areas for improvement, but it might not necessarily involve the direct observation of an employee's work or communications."	Valid type of employee work activity data being tracked	38
	Valid use case or purpose for tracking e.g. to measure productivity	21
	Synonymous with Monitoring and/or Surveillance	21
	Collecting Data	17
	Storing Data	10
	Analysing data	1
	Distinguishing from Monitoring and/or Surveillance	0
	Processing Data	0

Table 11: Tracking column analysis