Data subjects, digital surveillance, AI and the future of work

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)

PE 656.305 – December 2020

EN

Data subjects, digital surveillance, AI and the future of work

This report provides an in-depth overview of the social, political and economic urgency in identifying what we call the 'new surveillance workplace'. The report assesses the range of technologies that are being introduced to monitor, track and, ultimately, watch workers, and looks at the immense changes they imbue in several arenas.

How are institutions responding to the widespread uptake of new tracking technologies in workplaces, from the office, to the contact centre, to the factory? What are the parameters to protect the privacy and other rights of workers, given the unprecedented and ever-pervasive functions of monitoring technologies?

The report evidences how and where new technologies are being implemented; looks at the impact that surveillance workspaces are having on the employment relationship and on workers themselves at the psychosocial level; and outlines the social, legal and institutional frameworks within which this is occurring, across the EU and beyond, ultimately arguing that more worker representation is necessary to protect the data rights of workers.

AUTHORS

This study has been written by Associate Professor Dr Phoebe V. Moore, University of Leicester School of Business, United Kingdom, and Guest Research Fellow, Weizenbaum Institute, Wissenschaftszentrum für Sozialforschung, Berlin. The study was prepared at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

The author had assistance and contributions from AureolTM, Michael Bretschneider-Hagemes, Ian Brown, Amy De Bruycker, Christina J. Colclough, Craig Gent, Elena Gramano, Frank Hendrickx, Ehi Iden, Caroline Johansson, Sean King, Carol Landrino, Tone Lyse, Yonatan Miller, Patricia de Paiva Lareiro, Andrew Pakes, Bibiana Pinto, Mojca Prelesnik, Alison Powell, Gunn Robstad Andersen, Beryl ter Haar, Francisco José Trillo Párraga, Vincenzo Pietrogiovanni, Eliza Watt and Daniel Weidmann.

ADMINISTRATOR RESPONSIBLE

Mihalis Kritikos, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in October 2020.

PE 656.305
ISBN: 978-92-846-7280-6
doi: 10.2861/879078
QA-02-20-870-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (Intranet)
http://www.europarl.europa.eu/thinktank (Internet)
http://epthinktank.eu (blog)

Executive summary

Workplace surveillance is an age-old practice, but it has become easier and more common, as new technologies enable more varied, pervasive and widespread monitoring practices, and have increased employers' ability to monitor what seems like every aspect of workers' lives. New technological innovations have increased both the number of monitoring devices available to employers as well as the efficiency of these instruments to extract, process and store personal information. Digital transformation, work design experimentation and new technologies are, indeed, overwhelming methods with intensified potential to process personal data in the workplace. While much of the activity appears as an exciting and brave new world of possibility, workers' personal experiences of being tracked and monitored must be taken into account. Now, issues are emerging having to do with ownership of data, power dynamics of work-related surveillance, usage of data, human resource practices and workplace pressures in ways that cut across all socio-economic classes.

The first chapter of the present report 'Data subjects, digital surveillance, AI and the future of work', commissioned by the European Parliament's Panel for the Future of Science and Technology (STOA), deals with surveillance studies, which originates in legal studies and criminology but is increasingly important in sociology of work and digitalisation research. The first chapter outlines some of the technologies applied in workplaces. The second chapter looks at the employment relationship, involving how workers and managers, and surrounding pressures transform when a third actor (the machine and/or computer), is introduced. This chapter also covers the ways that inter-collegial relations are impacted, as well as issues around work/life integration.

The third chapter looks at data protection and privacy regulatory frameworks and other instruments as they have developed over time, leading up to today's General Data Protection Regulation (GDPR). Various historical moments have impacted how data and privacy protection has evolved. Concepts surrounding this legal historical trajectory have emerged, with some ambivalences at points around which philosophical and ethical foundations are at stake. Some of the tensions in legal concepts driving the debates in privacy and data protection for workers, and paradoxical circumstances within which they are seated, are then dealt with in chapter four, where the possibility for deriving inference from data can lead to discrimination and reputational damage; where the concept of worker 'consent' to data collection; and the implications for data collection from wellness and well-being initiatives in the workplace are increasingly under the microscope.

The fifth chapter outlines a series of country case studies, where applied labour and data protection and privacy policy are revealed. Many countries are reviewing data and privacy and labour laws because of new requirements emerging with the GDPR, which has also been extensively reviewed in the present report. Some legal cases have emerged whereby employers have been judged to breach data protection and privacy rules, such as Bărbulescu vs Romania. The sixth chapter, called 'Worker cameos', provides a series of worker narratives based on field interviews about their experiences of monitoring and tracking. In particular, content moderators and what the author calls 'AI trainers' are the highest surveilled and under the most psychosocial strain. Taking all of these findings into account, the seventh chapter provides a series of the author's suggestions for first principles and policy options, where worker representation and co-determination through social partnerships with unions, and more commitments to collective governance, are put forward.

Table of Contents

1. Surveillance workplaces and spaces, old and new

Workplace surveillance over time has occurred within a series of historical phases, where work design, labour markets, and industry trends have differed and business, social and labour processes have taken particular forms. Surveillance of workers can be both analogue and technological, and operates at a series of tangible and psychosocial levels. 'Surveillance and monitoring: The future of work in the digital era' was commissioned by the European Parliament Panel for the Future of Science and Technology to Primary Investigator (PI) Dr Phoebe V Moore in 2019. In the report on this nearly year-long project, we look at how insights in technological development have evolved within a sociological and business operations framework, and identify how technologies are being implemented to manage worker performance, productivity, wellness and other activities, in order to analyse and predict the social impact and future of work, within regulatory parameters. Workplace surveillance in the European Union is predominantly outlined, but as early, government-commissioned North American research into workplace surveillance was also very perceptive in foresight, some historical discussion of the United States' early activity as well as some insights from Norway and Nigeria, are included.

Workplace surveillance is not separate from the larger structures and systems of labour relations, management styles, workplace design, legal and ethical social trends and today, are explicitly part of the accelerating trends in digitalised surveillance in many spheres of everyday life. Therefore, we address all of these categories of analysis, alongside identifying where and how digitalised surveillance has and is occurring in workplaces or perhaps better said, work*spaces*, called as such because the concept of 'place' has to be interrogated and critiqued, precisely because work is carried out in an increasingly *virtual* spaces globally, and with the onset of Covid 19 working conditions, increasingly, in homes.

In 2017, a Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics clearly stated that:

> …assessments of economic shifts and the impact on employment as a result of robotics and machine learning need to be assessed; whereas, despite the undeniable advantages afforded by robotics, its implementation may entail a transformation of the labour market and a need to reflect on the future of education, employment, and social policies accordingly. (European Parliament 2017)

This Recommendation predicted that the use of machine learning and robotics will not 'automatically lead to job replacement', but indicates that lower skilled jobs are going to be more vulnerable to automation. Furthermore, the Recommendation cautions the likelihood of labour market transformations and changes to many spheres of life, including as above, 'education, employment and social policies' (ibid.). In this light, the current report builds on some of these earlier recommendations to the European Parliament, because it is now more important than ever to address the lagging discussions on ethics, social responsibility, social justice and importantly, the role of unions and worker representative groups in the continuous development and integration of technologies and digitalization into workplaces. The report is written with a human rights focus, seeing data privacy and protection as a fundamental human right.

Automation, robotics and artificial intelligence (AI) are part and parcel to the discussion of monitoring and surveillance of work, where a binding feature for how these processes emerge is the collection, storage, processing and usage of large data sets that are collected in more and more spheres of people's everyday lives and in particular, workplaces. A report prepared for the United Kingdom's Information Commissioner's Office (ICO) declared that 'we live in a surveillance society. It is pointless to talk about surveillance in the future tense… everyday life is suffused with surveillance encounters, not merely from dawn to dusk but 24/7' (Ball and Wood 2006). More than

one decade later, this statement could not be more relevant. From cameras at self-operated grocery store check-outs in New York, to facial recognition sensors at a local gym in London, to recorded calls with a call centre employee of banks who themselves may be based in India or Bangladesh, surveillance is an activity that is no longer only seemingly conducted by law officers on the streets watching out for robbers wearing balaclavas. People are watched in almost every corner of society, and sometimes people are even asked to watch one another, in what Julie E. Cohen calls a *participatory* surveillance (Cohen 2015). Gary T. Marx earlier referred to forms of participatory surveillance as a kind of 'new surveillance' in 1988, just as computers were becoming integrated into everyday life and seemingly integrating a new type of soft surveillance (Marx 1988). In 1982, Craig Brod had already warned of the dangers of over-use of computers at work and talked about the hazards of technostress resulting from the uptake of new technologies in everyday lives (Brod 1982).

Cohen, an established figure in the research arena of surveillance, looked at the issues surrounding privacy and systems of surveillance. Cohen argues that privacy, as a concept informing practices, has a bad reputation, where it has been touted as an old-fashioned concept and a delay to progress. Cohen counters these systemic assumptions and says that privacy should be a form of protection for the liberal self (2013: 1905) and important for the democratic process. Indeed, trading privacy for supposed progress reduces the scope for self-making and informed, reflective citizenship and a range of other values that are foundational to consumer society.

So, effective privacy regulation must render both public and private systems of surveillance meaningfully transparent and accountable, where privacy is defined in the dynamic sense: 'an interest in breathing room to engage in socially situated processes of boundary management' (Cohen 2012: 149, cited in Cohen 213: 1926-1927). Privacy incursions harm individuals, but not only individuals. Freedom from surveillance, Cohen argues, whether public or private, is foundational to the practice of informed and reflective citizenship. These ideas are important when looking at workers and their right to privacy. A reasonable expectation of privacy is likely when the actions of the employer suggest that privacy is a condition of work. Internationally there are variations in law and culture in terms of privacy, especially differences between the European Union and the USA. In Europe, privacy has tended to be seen as somewhat more fundamental, something that should not be forfeited, whilst in the US privacy can be viewed as a commodity (Smith and Tabak 2009).

There was a lot of discussion about business *culture* after Scientific Management, during the Human Relations and Systems Rationalism periods. Alder (2001) reviewed a range of organisational culture types, asking which ones are more/less amenable for electronic performance monitoring (EPM) integration. Right at the end of the latter period, Deal and Kennedy outlined four cultural types in 1982, which they argue are oriented around risk-taking and frequency of feedback within the organisation: '1) tough-guy macho, 2) work hard/play hard, 3) bet your company, and 4) process' (1982, cited in Alder 2001). Petrock, Alder notes, also outlines a typology of four organisational cultures: 1) clan culture 2) adhocracy, 3) hierarchy, and 4) market cultures (1990), but these types are limiting because there are no associated ways to measure or identify them, offered. Alder believes these delineations are incomplete and not fit for purpose. Wallach, however, came up with the best typology, Alder states, noting the signifiers within three types: 'bureaucratic, innovative and supportive' (Wallach 1983, cited in Ibid.). A bureaucratic culture is identified with hierarchy, regulation and procedure and is the organisational culture type that is most responsive and accepting of technological tracking. Alder (2001) argues that workers will respond differently to EPM in different organisational cultures. Therefore, Alder indicates that a management body that wants to implement EPM must think about the culture of their organisation to assess to what extent resistance to it will emerge, and how to accommodate this. These days, however, the culture-based arguments are less and less relevant, as metrics and data appear to hold the promise to make irrelevant specificities in qualitative differences and as data rights become increasingly mainstreamed across the consumer and worker spheres.

This report, overall, aims to highlight what kinds of technologies are being integrated to monitor, track and therefore, surveil workers; to identify how technologies are being implemented; to understand the impact that having new technologies in workplaces impacts the employment relationship; to throw light on the social, organisational, legal and institutional frameworks within which this is occurring; and reveal the institutional, legal and union responses. Finally, the goal of this report is to provide a set of first principles and policy options to provide EU member and associated states with guidance on protection the privacy and rights of worker data subjects.

Leading up to the General Data Protection Regulation (GDPR), the EU's Data Protection Working Party (Art. 29 WP) stressed that 'workers do not abandon their right to privacy and data protection every morning at the doors of the workplace' (2002: 4). Some degree of gathering and processing of personal data is a normal and in fact, a vital part of almost any employment relationship (Ball 2010). Some workers' personal data is necessary to complete contracts i.e. to pay workers and record absences, and much of it is both reasonable and justifiable for use by management. However, that is not to say that any and all forms of surveillance and data processing should be so considered.

Indeed, employers' surveillance practices must often be reviewed in light of concerns for the privacy or simply for the human dignity of the worker (Jeffrey 2002; Levin 2009), and this report sets out to do just this. The present author has already situated this trend within the contemporary pressures of global political economy pressures (Moore 2018c) and looked at the psychosocial violence and safety and health risks that workers face with the introduction of digitalised tracking and monitoring (Moore 2019, 2018b). Welfare state retrenchment and austerity policies alongside these technological interventions have coalesced into the 'political economy of anxiety' (Moore 2018a: 43) for workers, where self-quantification and wellness discourses and frames thrive, but structural economic change is not occurring fast enough with relevant protections and social partnerships with unions and other worker representative groups. Now, we set out the aims and intentions for the project which form each chapter.

The aim of the first chapter of the report is to review the concept of surveillance, where workplace electronic performance monitoring and privacy questions are increasingly important. The Taylorist employment model of mental vs manual work in a set hierarchy is increasingly a thing of the past, and while tools for measure were used in Taylor's workshops, the kinds of technology now available on the market have fed into significant differences to a new world of work. Parallel to this change, the pursuits for surveillance have entered more intimate and everyday spaces than before. The known categories of the 'watched' and the 'watcher' are transformed. 'New surveillance workplaces' or what we also refer to as 'workspaces', indeed, feature these new characteristics. The first chapter therefore looks at a range of new technologies which are contributing to the recent trends in an uptake of electronic monitoring and tracking at work, backed with existing empirical evidence and primary and secondary literature.

In the second chapter, the report's aim is to look at changes to a once presumed standard employment relationship, where managers and corporate and organisational hierarchies were explicit and clearly known. Now, management and operations processes are being digitalised, and workplaces are moving in to a myriad of domains. As a result of the changes to a more standard type of employment relationship and work environment, uncertainty or other psychosocial discomfort can emerge, where workers may feel their managers no longer trust them; or workers experience the issue of function creep, where data is used for other purposes than it was first collected for. Or competition between workers is intensified when performance data is viewable such as on the walls in call centre workplaces or on shared dashboards in gamified wellness programmes. The second chapter outlines the observable and documented as well as probable changes to the employment relationship which new technologies imbue.

The third chapter turns to the policy and regulatory frameworks and instruments surrounding privacy and data protection and technological tracking, starting with the Data Protection Directive.

The most important points in data protection and worker issue based policy are covered in the leadup to the GDPR. Interestingly, the International Labour Office's Code of Practice around workers' data, published as early as the 1990s, made similar interventions and recommendations that are now enforceable in the GDPR today. This chapter outlines this process and picks up on some of the most important and insightful developments to provide a foundation for the first principles and policy options outlined in later chapters of the report.

The aim of the fourth chapter is to identify some of the tensions in legal principles about which the present author has been concerned, where e.g. inviolability does not seem to cohere with the concept of power of command; or where inferences from data and the link to workers' reputations must be problematised. This chapter also looks at the concept of 'consent', which tends to be de-prioritised in discussions of the employment relationship (where consent is normally discussed in relation to a consumer, in the context of the GDPR) due to its already existing unequal nature. We argue that there are possibilities to rethink the definition of consent, nonetheless, and to perhaps look at a way to update the unidirectional conceptualization of this type of relationship.

The fifth chapter then provides a series of country case studies provided in part by a series of legal scholars from across the EU, and Norway and Nigeria, where contributors have outlined information about which technologies are characteristic in specific countries; identified which legal mechanisms are being used including aspects of labour law, to ultimately protect workers' privacy and data; looked at the ways local cases are working to integrate the GDPR as per Art. 88; and begins to put the focus on the role of worker representatives who, we ultimately recommend, should be considered meaningful social partners in dialogue with employers and with co-determination rights (see policy options).

In the sixth chapter, we present a series of 'Worker Cameos' which are based on semi-structured interviews carried out with a series of workers to identify where EPM and tracking are occurring and to investigate and identify workers' experience of this. Workers in many sectors and spheres, from dentists, to bankers, to content moderators, are being tracked. All workers interviewed feel that their work has intensified, expectations are higher, performance management is increasingly granular, and stress and anxiety are at an all-time high, as tracking and monitoring technologies become increasingly good at surveillance.

The report concludes with a set of first principles and policy options for European Parliament policymakers, prioritising the role of trade unions and other worker representative groups. These Principles and Options are designed to mitigate against the worst impacts of digitalised tracking, monitoring and surveillance in the world of work.

1.1. Objectives and methodology

A report of this size, relevance, and significance requires a sober and rigorous approach to data collection and presentation. Here, we outline the research practice tools we have applied for this project, indicating selected methods and approaches to firstly, carry out the semi-systematic literature review presented; secondly, prepare country case studies; and thirdly, carry out a series of semi-structured interviews with appropriate data subjects for this study. A detailed explanation of the report's objectives, and correspondent rationale and approaches for methodology selection and practice, are provided here.

The project adopts a mixed methods approach, conjoining primary and secondary literature review, case studies, and semi-structured qualitative interviews and analysis, to meet the objectives laid out in the Introduction. The author has adopted a grounded theory methodology for qualitative meta-analysis, meaning that she and researchers in her teams start from the investigative position even in the very first moments of research practice, with the explicit intention to draw out evidences and hypotheses based on semi-systematically gathered data and insights arising from the project

(Corbin and Strauss 2008), retaining theoretical sensitivity through a systematic approach to the secondary literature review, category building, semi-structured interviews, and reflection (Hoare et al. 2012). While the concept of meta-analysis originates in quantitative research, it is adapted within qualitative research to identify categorical relationships in a cumulative fashion. Seeking a cumulative development of what Stall-Meadows and Hyle talk about as 'theoretical research in their discipline' via 'induction, cumulative development, systematic analysing and interpreting data' (2010: 412) we adopt the core components of grounded theory development (Strauss and Corbin 1990). While the current report has not itself developed a new theory, as grounded theory researchers often do, the inroads are built for one, via systematic case study and literature review activities, with appropriate contextualising in the qualitative data from a sample of semi-structure interviews. The methods explained here indeed provide the foundation for a new theory of surveillance at work, that takes into account the categories identified as needing further research, such as the range of legal concepts and terminology that now require review due to new rules set by the GDPR.

The chosen methods outlined now have been designed to meet the objectives for this report, which are discussed here with supporting social science practice.

1.1.1. Literature review

The first objective of this report is to examine the various ways technology is used to monitor the modern workplace and the various social and technological forms workplace surveillance can take. This objective is founded in the semi-systematic literature review, where a detailed account of the wider reporting on where this is happening and how it is applied, is presented. The literature review provides a review of primary literature to identify the necessary policy and legislation background for relevant data privacy and protection law; and a review of academic literature to identify the debates surrounding the trajectory of relevant labour processes and business processing systems that led up to today's status quo of monitoring and tracking at work. To meet these objectives, the project involves not only a traditional academic literature review, but also provides an extensive policy and legislation and historical literature review to gain an appropriate policy background and framework, which itself has required extensive primary data collection and review.

Literature reviews require a thorough search of literature within specific chosen domains, quality assessment of that literature, synthesis, and reporting. In line with the report's objectives to look at how technologies are being used to monitor modern-day workplaces and to identify their surrounding social and technological forms, it is necessary to identify which bodies of knowledge and authors have written on these topics. Workplace tracking *itself* is not new and its analogue forms have a history even as far back as pre-war industrial betterment, where the technique to introduce specific spiritual and social norms into workers' everyday lives through education and housing arrangements (which were again magnified in the 1950s) allowed bosses a more intimate peek into workers' doings. Many management strategies have been trialed over time, but the academic debates really took hold in the 1980s when computational capacity allowed for the increase in electronic performance monitoring. Therefore, the report mentions the earlier analogue forms (albeit in a truncated form) before investigating more closely the debates in sociology and psychology looking at electronic and computational performance monitoring starting in the 1970s and continuing today.

To select literature for the review, a semi-systematic search method was selected. Following the approach carefully laid out by Booth, Sutton and Papaioannou (2016), Moore first identified review methods she would pursue in the planning phase of her approach to project management. Moore decided to apply a digitalised approach, selecting terms and categories to apply in database searches, searching for existing publications in high quality peer reviewed publications. Moore selected key search terms key and applied adjacency & proximity operators and used the Web of Science, EbscoHost and ieeeXplore. Categories included for example *electronic performance*

monitoring OR *EPM*, *worker monitoring* OR *workplace monitoring*, *worker surveillance* OR *workplace surveillance*. Moore also used other Boolean operators apart from 'OR' that are listed here, for example AND and NOT to identify appropriate terms. These articles narrow, broaden and eliminate sets that are researched by such databases as an aid to search the literature. On the basis of identifying relevant literature, Moore could heuristically, as well as based on identification of existing literature, identify the scope of her approach, which was to emphasise particular theoretical and empirical aspects of surveillance within historical periods of argument.

An aspect of this objective also requires a policy background report and thus, Moore carried out a search of policy materials and literatures discussing the relevant regulation in data protection and privacy as well as surrounding legal principles. Adding to the digitalised method, Moore used the snowball approach, which is to identify authors who are known within specific topics and policy and legal arenas and search for further work they have done to identify the materials needed. The literature review process involved a rigorous and careful quality assessment of the evidence located, based on fact checking and cross referencing (Booth, Sutton and Papaioannou 2016).

A further aspect of this objective is to shine light on how national governments, courts and international organisations have tried to determine whether and to what extent interference with the employees' private life is necessary or justifiable, and to what extent a fair balance is struck between the different interests involved. This objective is met by the extensive review of policy instruments and legal cases in chapter 3. The corresponding policy brief prepared alongside this report provides policy options that that are seen to be most likely to prevent a detrimental effect on workers and the employee-management relationship, slow down the perpetuation of existing inequalities in the workplace, result in increased worker input or at least an ability to contest the implementation of these devices, and in effect, to strengthen the protection of workers' rights and ensure that personal autonomy is guaranteed.

1.1.2. Case studies

The second objective of this report is to identify national cases that delve into the legal and institutional parameters within which electronic monitoring and tracking of workers occurs and to identify how a variety of different local governments have used relevant laws concerning monitoring of workers and surrounding data and privacy protections as well as the application of labour law. This is dealt with via a series of country case studies that are contributed to by a number of legal and health and safety experts in EU countries, Norway and Nigeria, who have outlined for Moore which laws have been applied in their own countries to deal with worker tracking and privacy questions. Case studies also identify governmental and social responses to misconduct or breach of contractual duties.

To further address this second objective, the following questions are also asked: where the scope of information, consultation, and co-determination rights exist for employee representatives in connection with monitoring of employees, how are they applied? Does the GDPR change the legal landscape sufficiently, when it comes to monitoring of employees? How will this new legislation impact the way that damages/remedies can be dealt with, in the case of employers who illegally monitor workers?

Case studies are the best social scientific method for collection of focused qualitative data on emerging trends within specific categories, identifying emergent trends and developing hypotheses and theories where literature reviews of primary and secondary data is complemented with new data on the appropriate topics, giving snapshots of a larger phenomenon. Robert Yin, perhaps the best known researcher to write about qualitative methods and an expert in case study design and execution indicates that the way to choose methodological tools is based on the research questions one is asking. He notes that 'what' questions are better suited with archival, text-

based research, or surveys, whereas case studies are better suited for 'how' or 'why' questions (Yin 2014: 10, 11).

Yin indicates that a case study is an empirical enquiry that 'investigates a contemporary phenomenon (the 'case') in depth and within its real-world context, especially when the boundaries between phenomenon an context may not be not clearly evident… you would want to do case study research because you want to understand a real-world case and assume that such an understanding is likely to involve contextual conditions pertinent to your case' (Yin 2014: 16, also see Yin and Davis 2007). Thus the legal and regulatory framework are identified in light of specific contextual conditions, allowing us to identify how and why the phenomenon of digital tracking is occurring and the ways in which governments are responding. The GDPR is a cross-national legislative tool that provides good approaches to protect workers from overuse of digital monitoring and tracking.

To deal with the research questions here and for data collection purposes, several legal experts in data protection and labour, and health and safety experts, across the EU as well as further afield, were approached, with the help of Elena Gramano, Frank Hendrickx and Laurent Pech. Legal experts supplied responses to the case study questions relating to this area of investigation. The questions sent to all legal experts were as follows:

1. What kinds of worker monitoring, tracking, and potentially, 'surveillance', prevail in your country?
2. Which industry/industries see the highest rates of worker monitoring?
3. In your legal system, what legal restrictions to monitoring workers are there?
4. What are the legal sources that recognize such prerogative?
5. Could such entitlement be assumed by means of other principles (i.e. property)?
6. Is there any case law on the issue? If yes, what are the main principles elaborated by courts in order to regulate/limit the employer's surveillance in the working place?
7. Are there any examples of misconduct and breach of contract on the part of the employer with regards to violation of tracking and monitoring of workers?
8. What is the role of workers' representatives in the regulation of the surveillance on the working place?
9. What is the role of workers' representatives in the implementation of such regulation?

Respondents were invited to respond to these questions and Moore used responses to prepare each Case Study. Data analysis involved careful reflection of responses in a reflexive manner and in some cases, continued dialogue with respondents.

1.1.3. Semi-structured interviews

The third objective of this report is to map the main concerns that workers have about surveillance at work and how it is being carried out in various workplaces/spaces beyond typical environments such as call centres and factories, where location tracking, biometrics and a whole slew of new forms of covert surveillance have very relevant consequences for workers. Well-being, work culture, productivity, creativity and motivation are all potentially impacted. The experiences of workers themselves are important in a variety of industries, because monitoring and tracking occur across the board and it is important to gain a broad range of insights.

The objective here is also to examine the effects of these surveillance methods/practices upon the privacy and dignity of workers; to focus on the analysis of the controlling aspect of monitoring; and to look at any negative impacts of these surveillance practices upon the employer-employee relationship and the protection of human rights. This objective is met via the rigorous and semi-systematic literature review in chapter 1, where across a range of disciplines, academic literature has looked at the possible impacts on workers as well as outlined cases where workplaces and workers' experiences have been systematically researched (see Moorman and Wells 2003; Sewell et al. 2011; Stanton and Julian 2002; Grant and Higgins 1989; Griffith 1993).

However, for the purposes of the current report, current experiences based on new material are important to identify given the recent introduction of further types of technologies into this arena as well as media publicity surrounding the impact of high surveillance environments such as seen in content moderation workplaces, on workers (Newton 2019a, 2019b). Therefore, Moore identified semi-structured interviews of a series of workers as a way to gather appropriate and rich data identifying workers' experiences. Semi-structured interviews are an established method in social science research, usually chosen when the researcher intends to:

- Gather facts, attitudes and opinions.
- Gather data on topics where the interviewer is relatively certain that the relevant issues have been identified, but still provides users with the opportunity to raise new issues that are important to them through open-ended questions.
- Gather data when you cannot observe behaviour directly because of timing, hazards, privacy or other factors.
- Understand user goals.
- Gather information about tasks, task flow, and work artefacts such as job aids, forms, best practice documents, workflow diagrams, signs, equipment, photographs, and posters.
- Gather data on complex issues where probing and clarification of answers are required. (Wilson 2014: 24, 25)

Research assistants worked with Moore to interview ten workers in all, consisting of two content moderators, whereby content moderation is currently seen as one of the most grueling jobs and most heavily surveilled, in digital work (Gray and Suri 2019; Roberts 2019; Gillespie 2018); two call centre workers in sales and management, where call centre work has been consistently understood as a highly monitored and performance monitored environment (Bain and Taylor 2000; Poster 2018; Woodcock 2016); but other industry workers who are usually not researched, which provides a good counterweight and a more balanced as well as broadly based analysis of workers' experiences. This includes one consultant for an international organisation; a dentist; a creative director; and a financial analyst.

The report does not set out to provide grand narratives with broadly based statistical relevance, but rather, to provide in-depth snapshots of people's contemporary experiences, which is an appropriate data gathering method in the grounded theory research process. All interviewees signed consent forms indicating that the textual data gathered by the interviewer would only be used for the purposes of the current report and that they consent to this occurring.

Because of the nature of the sensitivity of this kind of discussion, and indeed most discussions about personal experiences, the social-psychological setting of the interview was relevant. Moore held specific discussions with interviewers before they went into the field, to ensure they set up the environment appropriately and thought about a range of matters. Interviewers considered their own role in potentially influencing the environment of the question and answer session itself.

Furthermore, interviewees process questions differently depending on social status, impressions of cost-benefit and other cognitive as well as emotional and subjective positions. Atteslander (2008)

recommends consideration of this when preparing for interviews and developing sets of questions. People may interpret questions differently, may respond to the interviewer in various ways and may have a variety of unspoken concerns likewise. The way that an interviewer can be sensitive to this is to listen and be as open to the speaker as possible; to not steer responses; to be reflexive and open. Analysis begins as soon as the interview begins, unlike some forms of social science research, and this is furthermore carried out in dialogue between researchers on projects (Stall-Meadows and Hyle 2010).

The questionnaire was prepared by Moore (see Appendix I). Forming the grounded theory approach, questions were organised in the categories: metadata, phenomenon, causal conditions, intervening conditions and consequences. Responses were used to create what she has called 'Cameos', which are detailed descriptions of each workers' experience. From this data, analyses are then drawn up which compare experiences.

Now, we focus on the concept of surveillance and its intellectual heritage and identify how it is used in academic writing to look at work.

1.2. What is surveillance?

The concept of *surveillance* has a long history in its own right, in discourses of justice, policing and intelligence. The word is from French, where its etymology stems from the Latin word *vigilare* meaning to supervise, monitor, guard, and keep an eye on. But today, we may reminisce about the old days when surveillance was only carried out for catching criminals and ne're-do-wells. The 'criminal' is no longer a known category a priori, but can even be derived and emerge from the practices of surveillance themselves. French philosopher Foucault warned us of the ways that *too much* watching, or watching that is too invasive, could result in new labels of criminality. Foucault applied Jeremy Bentham's concept of a certain kind of prison design, the 'panopticon', which is where a watch tower sits directly in the centre of a circular prison, and the wall-less cells face inwards. One cannot even know if someone is sitting in the central tower, nor whether other prisoners in their cells are watching from across the prison courtyard.

The metaphor of the social panopticon is that surveillance does not only involve a known watcher who is seeking out e.g. suspected deviants who are perpetually in hiding, in a cat and mouse game, but that society becomes structured to induce all of us to watch each other. Surveillance is no longer something that happens to other people. Surveillance is all around us. The watcher becomes the watched, and people are pitted against each other through various methods. We are expected to watch one another for misdemeanors as well as to start watching ourselves closely. This is an exercise of what Foucault calls 'biopower', which refers to the expansion of the arenas of orientation of where surveillance security practices are necessary, where psychology and human behaviour outside the 'ten commandments' styles of judgement become increasingly examined. So it is not only the subject who is under scrutiny, but the objectification and abstraction of people's behaviour which are turned into quantified datasets, and the methods of measuring become political. Even people's biological conditions become an arena for investigation, where *biopower* is a 'set of mechanisms through which the basic biological features of the human species became the object a political strategy, of a general strategy of power' (Foucault 2007: 1). Foucault's ideas inform some researchers who write about workplace surveillance, as well as Deleuze (1990), such as Erwin (2015), who explains the ways that contemporary surveillance techniques create people's data doubles.

Law enforcement and financial industry databases for example, categorise and encode data, and predictive algorithms are then used to predict future behaviour. Erwin refers to Deleuze's concept of surveillant assemblages, where individuals are then categorised and groups themselves become larger ensembles. Deleuze also theorises a 'control paradigm' which accounts for some key features of today's digital surveillance methods. Foucault and Deleuze are very influential in many schools of thought, but they are by no means the only philosophers nor theorists to influence surveillance researchers.

The author of the current report is a sociologist and has tended to arrive at specific perspectives through a socio-political lens, but clearly there are a variety of voices in surveillance at work debates.

Organisational and industrial sociologists, data scientists, philosophers and occupational and organisational psychologists, write about workplace surveillance from different epistemological and ontological foundations. Even as far back as 1905, before Taylor had published Principles of Scientific Management (1911) researchers were looking at the ways that performance feedback impacted workers (Judd 1905). In 1986, Siegel et al. predicted that computer-mediated communication would become endemic and ubiquitous within organisations and would impact how feedback is given to employers (1986). But not all researchers view this as a positive development. Indeed, researchers in the field of sociology such as Mathiesen (1997) and philosophy such as Erwin (2015) have looked at monitoring of workers and their responses and the frameworks within which these practices sit, tending to portray workplace surveillance in a dystopian light. Authors who view surveillance at work negatively in this way have been significantly influenced by Foucault. Joseph Weizenbaum; who invented the predecessor to the chatbot, Eliza, and is known as one of the first critical AI researchers; had warned of the dark sides of technological integration and even warned that 'time after time, science has led us to insights that, at least when seen superficially, diminish man' (Weizenbaum 1972: 610).

Of course, the negative angle is only one side of the argument. How does one achieve control, without controlling, or at least, appearing to control (Sewell 1998: 403)? The panopticon operates based on workers' self-control and discipline, where e.g. the organisation's 'values' are embraced and upheld by workers and their behaviour and subjectivity is modelled around them. Another management method is identified by organisational sociologist Sewell who pondered the paradox of the introduction of teamwork and peer surveillance in the 1990s alongside intensified hierarchically derived disciplinary models with the use of information technologies, to identify a new model of industrial labour processes which incorporates both vertical and horizontal forms of surveillance (Sewell 1998). So workers begin to surveil themselves and their peers in these frameworks. Poster refers to electronic surveillance as leading to a 'superpanopticon', whereby an unobtrusive surveillance superstructure, based on language and symbols, has been created which impacts most, if not all areas of life, including the workplace (Poster 1990).

Other researchers during this significant time period of the 1980s and 1990s build on Foucault and other researchers, innovating such concepts as dataveillance (Clarke 1987), panoptic 'sort' (Gandy 1993), and electronic panopticon (Lyon 1994). Later researchers discuss lateral surveillance (Andrejevic 2005), social searching (Lampe et al 2006), social surveillance (Joinson 2008; Tokunaga 2011), and liquid surveillance (Baumann and Lyon 2012).

Non-academic publications use terms such as participatory panopticon, virtual panopticon, digital panopticism, omniopticon tool, and social media panopticon (see Romele et al. 2017).

Psychologists have tended to write about workplace surveillance from a neutral position, where the discussions are around how monitoring happens and what the cost ultimately is, without political overtones (Ball 2010: 88). Data scientists Stanton and Julian (2002) argue that social information processing theory, adapting Salancik and Pfeffer's theory (1978), can be useful to develop predictions about task performance in electronic performance management.

There have also been a range of discussions of various categorises of surveillance as being on the one hand, hard surveillance and on the other, soft surveillance. Electronic surveillance is described as 'hard surveillance' by Sewell, which Thompson states has 'moved beyond the coercive, personalised and non-rational elements of such arrangements, as well as being more intensive, powerful and unobtrusive' (Thompson 2003: 139). Thompson cites Zuboff's earlier work to describe a 'soft' surveillance (Zuboff 1988). This perspective views the panopticon in a kinder way, as something that allows 'shared custodianship' of the surveillance. Zuboff instead argues that the technology promotes a *learning* organisation and that it actually helps promote progress within an organisation.

Zuboff identified in the 1980s a range of alternative futures for work and power in the age of the smart machine. The collection and use of information and data permits automation or something she calls a practice of 'informate'-ing. The latter would provide better meanings for people to understand and perhaps even enjoy work, with experimentation and creative collaboration. Automation of information however, leads to a road of entrenched Taylorism. Thompson argues that there has been a shift towards more surveillance practices in business, there is not enough evidence to conclude that a combination of a panopticon and peer pressure is effective enough to 'constitute a new model of control of the labour process' (2003: 138). Indeed, Zuboff now discusses 'surveillance capitalism' (2019) to position the debates within that conversation.

Gary T. Marx also wrote in the year Zuboff published her important earlier piece on what he called 'new surveillance' (1988), where the 'watched' can be anyone, and 'watching' can occur ubiquitously and for any reason. New technologies for these practices can involve computer matching, profiling and data mining; computer and electronic location monitoring; DNA analysis; drug tests; brain scans for lie detection; various self-administered tests and thermal imaging, or 'imaging to reveal what is behind walls and enclosures' (Marx 2005). The innovation in new surveillance, he wrote, is that it can be carried out with better known 'geographical places and spaces, particular time periods, networks, systems and categories of person' (Marx 2002: 10), rather than historical versions where it was based on specific, usually known, people and where location tracking occurred through James Bond style physical following and surreptitious analogue tracking and identification. Today, advances in computation create a very new landscape for accurate identification. Far more types of data can be gathered computationally than ever before, very quickly and systematically.

We can find, even from over a decade ago, examples of employees' recognition of the potential for bosses being able to store past information about worker performance and behaviour, and put it to use selectively. In 2007, an interviewee made a remarkably blunt comment:

> As we go forward, we start to gather all types of information about people because saving information is cheap. The problem is that when I want to catch someone or not hire someone, I can go back and then gather all this information and create a case against anybody I want. That is very, very dangerous. (Allen et al. 2007: 190-191)

Therefore, as we see, workplace surveillance as a subject of investigation for sociologists and other researchers is not *itself* new, although worker surveillance has been called the 'Cinderella sister of surveillance studies' (Edwards et al. 2018: 17). However, an increasing interest in the topic over recent years is clear, and Cinderella is finding her proverbial shoe. These are some of the reasons that that the topic has maintained and is gaining relevance. Now, the intensification of the surveillance in workplaces and business operations is driven by ever-evolving technological changes, allowing the gaze of the supervisor, the gaze of fellow workers, and the internal eye cast over the self to take new digital forms. The broadening of the scope and depth of possible workplace surveillance is evident, now with abilities to observe and scrutinise aspects of workers' lives which were previously inaccessible (Thompson 2003; Moore 2018a).

Ravid et al. (2020) provide an excellent review of electronic performance monitoring literature and a typology of research that brings the debate into a contemporary recognition of the fact, authors argue, that monitoring must be studied alongside the psychological characteristics of use and the purpose for electronic performance monitoring enactment. Referring to Stanton (2000) who had earlier carried out a similar review (see Appendix II), these authors look at the ways in which 'traditional monitoring' have moved more to a 'psychological level'. Behavioural details can now be captured at levels previously unseen. Therefore it is increasingly important to reveal what impact these new trends are having on workers, as the 'Medusa stare' may turn workers into metaphorical stone statues (Wallach 2011), unable to function at their best capacity, as arenas of some privacy and autonomy are systematically eliminated.

The following chapters describe what is at stake in the contemporary workplace of surveillance. The areas outlined are 1) a history of the labour and business processes which led up to today's rise in the application and use of monitoring and tracking technologies; 2) the types of technologies applied in new surveillance workplaces and spaces; and 3) the ways that new workplace surveillance is impacting employment relations within the workplace, or what academic researchers have called the employment relationship.

1.3. Business processes and technological surveillance at work

Perhaps the roots for modern surveillance lie in its pre-modern forms, alongside the birth of the American factory in the mid 1880s. The USA was founded on the spirit of individualism and self-sufficiency as well as religious puritanism. During the period of Industrial Betterment in the 19th century, masses of European workers moved to the United States to work in the factories and brought with them, so the story goes, European values of cooperation and partnership were re-introduced. A groups of clergymen and intellectuals recommended providing spiritual guidance for working people and the YMCA was founded during this period precisely for the industrial working class to provide moral guidance during a period when huge numbers of people were needed to facilitate rapid early industrialisation through intensive manual labour. Pre-modern workplace management over large clusters of people in factories, then, during this period of early work design period, reflected the value of the church.

But as modernity took hold with the intensification of industrialisation, convictions of a rational actor *without* a spiritual dependence; efficiency as imperative; and the desire for a compression of space and time became evident within 'machine-based capitalism' (Staples 2014: 20). During this period, perhaps the most famous work design gurus of all time Frederick W Taylor, Frank Gilbreth and Lillian Gilbreth, popularised the notion of the 'one best way' for production, which started with human movements in factories and moved into thinking about how to organise societies. Alongside the desire for a model of perfectly productive human movements and perfectly efficient social structuring came an extreme desire for rational micro-management via measure, where various early instruments such as a micro-chromometer, stethoscope and early cameras were used to record people's movements and measured against productivity scores. Even during this early period, technologies were considered useful to survey workers' activities and behaviour and data used to make decisions about workplaces.

Barley and Kunda published an important paper in 1992 that outlines managerial discourses around ideal methods to control the workplace, in historical blocks until the 1990s (Barley and Kunda 1992), where there are variations in normative and rational rhetoric over time. The Industrial Betterment phase was seen to be 'normative', but during the scientific management phase, 'control' and 'rationality' took hold. Scientific management, with its early iterations of workplace surveillance, lasted for about 25 years before the Human Relations (normative) period 1925 - 1955 gave way to Systems Rationalism (rational) from 1955 – 1980. It is during the Systems Rationalism period that computational sophistication advanced most explicitly. Mathematicians, physicists and statisticians,

who had been called upon during the second World War to apply computation to logistical planning, were invited to design ways to use computational methods to define workplace operations. Indeed, the Operations Research Society and Institute for Management Science, were established to identify ways to apply quantitative methods based on digital computation, to management.

By September 1987, the report 'The Electronic Supervisor: New Technology, New Tensions' was published by the Congress of the United States Office of Technology Assessment, to lay the groundwork for thinking about computer-based workplace monitoring, and the early stages of a shift to a post-industrial, information based economy and society. This early study was analytically insightful, outlining not only where tools for supervising office activities were already in place and what their likely future might be, but also refers to the implications for workers' privacy, fairness and stress, as well possible issues surrounding how and where usage for worker data accumulated, could occur. In the 1980s, the highest rates of computer-based monitoring occurred in telephony, where the software and hardware for telephone call accounting was a rapidly growing area in the telecommunication industry. 'Service observation', the US Congress authors indicate, is where workers' telephone calls were observed clandestinely by a manager in order to assess courtesy and accuracy. This type of appraisal would possibly fulfil the expectations of what we could call today perhaps, a 'human in the loop', although workers were not aware of when managers were listening to their calls. But 'telephone call accounting' allowed management to gather data about both the *duration* and the *destinations* of calls. That quantifiable information was recorded automatically. The rationale for this type of disruptive computer-based monitoring could be used not only for monitoring of work processes i.e. to identify how long workers were spending on calls and who they were telephoning, but to oversee financial costs to the company, during a time when telephone lines and services were regularly billed and such things as 'wireless fidelity' and 'wireless internet' were hardly imagined.

The 1987 US Congress report provided insights into the precipitous learning curve for managers, workers and customers alike, in that it outlines how a rapidly emerging phenomenon of workplace practices might be a foreshadowing of future uses of computer-based technologies to monitor, in particular, office work. Managers, the report indicates, tend to favour computer monitoring, because it helps with productivity enhancement, plan personnel, aid with equipment need identification, and spot bottlenecks. Workers, however, may fear they are being spied on or will suffer from lowered dignity, autonomy and reductions of privacy. Hidden telephone call intervention could also lead to customers' reduced privacy. 'Minute-by-minute records' (US Congress 1987: 5) kept by managers could be used to force people to work faster and otherwise be used in appraisals and staffing decisions. Workers might experience 'unfair' or 'abusive' monitoring, where allegations might focus on increased quotas, punitive usage of data or 'inappropriate work standards' (1987: 1).

This foundational report, although a telecommunications-focussed North American artefact, is fascinating because it outlines the work processes, legal landscapes, and labour force tendencies within which an increase in computer-aided tracking and monitoring was occurring in the 1980s. In 1987, women had entered the workplace and constituted approximately half of the workforce. There had also been a growth in clerical employees from 5 million in 1940 to 20 million in 1980. Nearly 1/3 of women working in the USA at that time were in clerical settings. While automation had been primarily evident in manufacturing, automation within the office setting rose in the 1970s and 1980s. Computers started to become common in offices in the 1980s. Technologically aided tracking activity occurred in office-based work and reflected repetitive tasks, the US Congress report noted, and thus, women were the most impacted by this trend. While simply having a computer in the office does not automatically lead to worker surveillance, in 1987, 6 million US workers were electronically monitored, 40 million US workers were seen to be subject to electronic monitoring and as many as 75 per cent of large companies electronically monitored their workers (Alder 2001: 323). While companies had been monitoring workers for centuries, the new forms of EPM starting

in the 1980s were seen to be different, as they are 'constant, pervasive, and unblinking' (Ibid. 324). The debates in the pros and cons of electronical monitoring really took hold during this period. Proponents claimed that it would improve productivity as well as staff morale and employee satisfaction (Aiello and Svec 1993; Griffith 1993; Marx 1992; Nebeker and Tatum 1993) and its opponents indicted almost the direct opposite, e.g. that it would reduce job satisfaction, increase stress, invade consumer and worker privacy, lead to worker 'speed up', and result in eroded teamwork (Ross 1992; Grant, Higgins and Irving 1988; Sanders 1990; US Congress 1987). Aiello and Kolb (1995) ran a test to look at the variations in how high-skilled workers will perform when monitored, in comparison to lower-skilled workers. The results demonstrated that highly skilled performers improved scores when monitored, compared to those who were not; but that lower-skilled workers who were monitored, performed worse than their counterparts. Authors of this classical study argue that the social facilitation framework (Zajonc 1965) has an effect on results and that familiarity and cohesion across groups creates variable patterns. While there are some good studies like this one, debates were nevertheless based on relatively scant data, often anecdotal and light on empirical rigour. Nonetheless, given the importance of this shift and the rise in the debate during this period, it is notable that collective bargaining was largely absent. Some quality of work committees met in workplaces to facilitate dialogue on these issues. What would the future be, for 'minute-by-minute' recording of workers' activities?

While the original discussions about workplace surveillance were in the 1980s, they picked up again in the late 1990s and first decade of the 21st century. In 2010, Ball reported that surveillance in workplaces was developing in three areas: 1) The increase in the use of personal data, 2) biometrics, and 3) covert surveillance. Ball argues that changes to workplace systems, or what she calls 'Human Resource Information Systems', characterise this new rise in methods, and that the shift in these trends is that internet-based, or e-recruitment during this period, has shifted some parameters for the use of technologies. In 2004, she argues, only seven per cent of recruitment, at least in the UK, was internet based. This started to advance, however. The USA stored 20 million curriculum vitaes (CVs) and in the 2000s, the e-recruitment industry was linked to the second-largest source of income made via the internet, after pornography (Ball 2010: 91).

However, regardless of their technical capabilities and potential, surveillance technologies are implemented within complex social contexts and sit within specific and changeable business processes and operations, and so are not determinate, but will always partially depend on the properties of these contexts as well as on people's reactions to the technology. The hopes and expectations of management teams are usually that data collection and processing will lead to increased productivity and better performance of staff, but empirical evidence also suggests such monitoring practices can have the opposite effect. Surveillance can be counterproductive for productivity, increase absences from work and create an atmosphere of hostility and feelings of mistrust (Sarpong and Rees 2014). Some employees have said that they feel as though they are being treated like children when monitoring systems are implemented (Lim 2002). Alder shows there is evidence for monitoring having impacts in both directions, in some cases increasing, and in some cases decreasing productivity (2001, 2007). Data collection in the work context can demonstrate managers' attempts to produce objectively reliable data sets that can then be used to make reliable decisions, but as this report will indicate, the human response is not objectively defined, is increasingly evident, and is now more than ever, in fact, necessary, to ensure human/computer interaction remembers the primary importance of the human.

1.4. Technologies of new surveillance workplaces and spaces

The Trades Union Congress (TUC) reported in 2018 that the top methods of workplace surveillance are:

- Phone logs and calls
- Recording calls
- Monitoring emails, files and browsing histories
- Cosed circuit television cameras (CCTV) (TUC 2018, also see UK Case Study below)

The first two forms of tracking and monitoring practices are older than the final two, where 24 hours, 7 days a week, recording possibilities now exist that are both visual recordings of human activities and data gathering in the backend of machines used for work. This TUC report indicated that many new forms of workplace surveillance are being trialed or used more intensively, including facial recognition and wearable devices that can track many aspects of human biological activities as well as track the conditions of their working environments.

The workplace monitoring software industry, also called the 'employee monitoring *solution* industry', is predicted to reach 3.84 billion USD by 2023 (Market Research Future 2019) and was said to be booming even in 2016 (Rosengren & Ottosson 2016) and on the rise in 2009 (The Economist 2009). *PC magazine* lists the 'best employee monitoring software for 2019', where software offers such activities as stealth monitoring, live video feed, remote desktop control, document and file tracking, keyword tracking, optical character recognition, blurred screenshots, automated alerts, keystroke recording, location tracking and user privacy settings (Marvin 2019). Hardware, including armbands, data glasses, and assistive devices also collects data about such things as movement, breaks taken, accuracy and productivity scores.

Selected datasets are created from these extractive mechanisms, which are then fed into algorithmic equations to answer specifically designed questions by management. Some forms of surveillance are continuous, such as key logging and phone recording, while others can be time-limited, once-off, or periodical in their activity (Rosenblat et al. 2014). There is facial recognition technology that is being trialled to automatically recognise and record workers' emotions, apps that rely on data collected by accelerometers in employees' mobile devices, and systems that gather and organise staff's social media usage (Ball 2014). The raw data collected of the various activities can then be fed into increasingly complex modelling systems and used construct behavioural profiles, patterns and benchmarks. Such standards and the possibility to constantly revise them and use them for comparisons allows management teams to detect when someone is deviating from the norm, whether that be their own norms, or that of some group.

New monitoring technologies are vast in number and functionality and are constantly being invented, so the current report cannot cover all of them, but some types are used every day already, such as the tracking and recording of computer and phone activity, global positioning system (GPS) tracking, CCTV (which are sometimes covert), and electronic recruitment systems (Ball 2014) in people analytics, discussed in the Algorithms section below. While we do not yet know completely in which ways they will be implemented and for precisely what they will be used in all cases, current evidence of the practices of digitalised tracking, monitoring and various methods for collection and processing as well as uses of data are now outlined, to give some insight into new surveillance workspaces and the future of work.

1.4.1. Algorithms

One of the most important tools in the contemporary world of surveillance and the workspace is the algorithm, because this computational tool has a new competence linked to the availability of big data sets that are used to train machines to learn. This is what makes contemporary algorithms

distinct from other workplace technologies used over time as well as sets them apart from the flow chart like mathematical processes that define earlier algorithms.

While once, companies deleted data because investment in storage was seen as a luxury, but now, they cannot get enough of it, and are even actively generating it. Indeed, peak algorithm is perhaps underway, in part because of the existence of very big data sets that are collected and curated by companies, public institutions, banks, police, and medical facilities over the last decade. Data collection is standard practice by seemingly all institutions and organisations. The difference now is that bit data is fed into algorithms which can *themselves* make decisions, because in their pure form, algorithms are fully automatic and appear to have intelligence which in part has led to the current hype around AI in workplaces (Moore 2019). Where some systems might have obvious deliniations or end points for what data is necessary and at what point data collection should terminate, Bloom highlights the fact that there is no clear end-point to data collection at work (Bloom 2019: 9). The worker, management and human resource infrastructure triage has been disrupted and transformed, seemingly irreversibly, with the introduction of ever-sophisticated algorithms. It is as though an entirely new actor, with agency of its own, has entered the workplace and the employment relationship, but this actor is ultimately, a machine rather than a human.

An algorithm is a set of rules used for computation. Dourish explains that:

> In computer science terms, an algorithm is an abstract, formalised description of a computational procedure. Algorithms fall into different types according to their properties or domains – combinatorial algorithms deal with counting and enumeration, numerical algorithms produce numerical (rather than symbolic) answers to equational problem, while probabilistic algorithms produce results within particular bounds of certainty. (Dourish 2016: 3)

While they are in the first instance a tool, discussions in social science literature tend to look at how algorithms are used in the social world to provide data that is then used for various decision-making purposes, from likelihood of recidivism, ability to pay off debts and some medical purposes. This is what gives algorithms a kind of social power (Beer 2017). Beer assesses the functions of algorithms, demonstrating how they are deployed, and then explores how the idea of an algorithm itself plays a role in social ordering which reflects a 'calculative objectivity'. The author then comments that the issue facing social scientists is 'the potential difficulty of fully appreciating the object of study' (2017: 17). It would be inaccurate to separate algorithms from the social world however, because algorithms themselves *are* the decision-making parts of code, which is particularly relevant when machine learning is applied to such algorithms. Therefore, it becomes difficult to disentangle an algorithm from organisational decision-making. Moore (2018) and Waters and Woodcock (2017) critically discuss algorithmic management and Prassl (2018) defines the 'algorithmic boss', where numerical figures are derived from a wide range of new sources and used to make decisions about workers and job candidates alike.

Colman, Bülmann, O'Donnell and van der Tuin discuss the 'algorithmic condition' which haunts modern societies. Drawing from Arendt's 'active life' and Lyotard's notion of 'computerised societies', this European Commission report is critical of a reliance on algorithms and coding to reflect reality (Colman et al.: 2018). Data collected from new technologies is not only used to look back and evaluate past performance, or monitor workers in real time, but is now also being used as a fuel for algorithms that also help users make predictions about the future (Edwards et al. 2018). Examples include electronic recruitment, promotions and dismissals, where major decisions can now be made by these algorithms without human input, often based on data collected through intense electronic surveillance. These algorithms are using data previously collected electronically, but the data may have been shown to be biased and having errors that result in discriminatory outputs (Noble 2018; O'Neill 2016; Cherry 2016). It is not only that the predictions and results produced by these algorithms can be unfair and incorrect, but the fact that they are so opaque,

sitting within a black box (Moore and Joyce 2020), means it is almost impossible for employees to understand them, let alone openly challenge their findings (Edwards and Veale 2017).

Many aspects and dimensions of computer usage can be observed and recorded by monitoring technologies: the names, location and contents of files stored and websites visited, the words spoken on digital communication channels such as messaging services and email, what was typed on a keyboard, when and for how long somebody was active at their keyboard, and what sort of content was posted to social media (Schumacher 2010). Adding to this, the number of keyboard click strokes, fingerprints, logins to computer terminals, tone of voice, and so on, can be identified, aggregated and processed via algorithms, where data and its interrogation inform business operations and for human resource decision-making. Some aspects and features of these technologies are identical to those used by parents to monitor their children's internet and computer usage (Rosengren and Ottosson 2016). Now, the use of machine learning and AI augmentation become the final frontier of these investigation processes where vast amounts of data that is more intensively collected than ever before, can be used to create large datasets that are used for cross-analysis of behavioural and identification trends at work.

Edwards et al. present a five-stage model of surveillance in society, with the current era being 'Surveillance 5.0: the Age of the Algorithms' (Edwards et al. 2018). For them the latest important development has been the introduction of machine-learning and algorithms to the surveillance process. These are used in association with, and on top of, the already detailed data and information about employees that has been collected electronically. Using the metaphor of the panopticon, Edwards (et al.) talk about how algorithms are used to detect patterns and trends in data and to categorise and profile workers. As well as this algorithms are now also being relied upon to make important decisions such as hiring, firing and promoting workers, and they play a central role in real time surveillance of workers' emotions and behaviours (2018: 9-11).

Indeed, now, huge swathes of data are made available for management teams to make calculations and analysis via algorithms. Levy carried out a case study looking at truck drivers and the data collected about their work, and indicated that the company appeared to believe that comparisons along '[any] imaginable axis of variation' (Levy 2015: 166-167) would be possible. In her case study, data about drivers' performance and activity was shared across colleagues in order to create inter-group competition, which was in line with the messages and advice from the companies selling such software. The companies producing such technology probably understand that there may be resistance from those being put under surveillance, and the accompanying manuals for tracking technologies often recommend that employers make a 'culture change' and start to appeal more to people's inherent tendency towards competitiveness as a method to overcome resistance to the adoption of the technology (2015: 170-171).

Yeung discusses 'algorithmic regulation' as exemplifying:

> …decision-making systems that regulate a domain of activity in order to manage risk or alter behaviour through continual computational generation of knowledge by systematically collecting data (in real time on a continuous basis) emitted directly from numerous dynamic components pertaining to the regulated environment in order to identify, and if necessary, automatically refine (or prompt refinement of), the system's operations to attain a pre-specified goal. (Yeung 2017: 1)

In other words, big data is first gathered from workers, where longitudinal data is obtained from specifically selected data silos. Data is then used within equations designed to identify specific patterns, regularities and irregularities from that data which produce answers to specifically targeted questions about workers. The surveillance possibilities of the usage of algorithms in the workplace, where they are applied in people analytics, platform work, warehouse work and more, are significant, because surveillance is based on the idea of truth-finding missions, as discussed in

the first chapters of this report. French philosopher Michel Foucault's 1976 lecture series on the production of truth, and the 'how' of power in that process, is very useful for critiquing the ways in which algorithms are seen to produce reliable 'truths', based on calculation. Algorithms seem to produce truth via:

1) the material interventions algorithms make, and

2) discursive interventions concerning algorithms. (Beer 2017: 8)

This second method of truth creation reminds us that, in fact, only *certain* truths are cultivated, truths that are intended to influence or convince, as well as control. This demonstrates a certain rationality based on 'the [perceived] virtues of calculation, competition, efficiency, objectivity and the need to be strategic' (2017: 9) (italics added by current author).

For algorithms to be useful in decision-making, objectivity must be assumed, which is a serious issue considering the black boxes within which they sit, i.e. the surrounding obfuscated processes and sometimes unpredictable or assumed to be inaccessible complete knowledge, upon which they are designed and derived. O'Neill (2016) and Noble (2018) have written in depth about the ways that algorithms have led to discrimination, where the data itself reflects historically discriminatory practices. Computerised decisions have an 'air of rationality or infallibility and people might blindly follow them' (Borgesius 2018: 8). However, the processes that function to decide relevance of datasets in relation to the solutions sought, are often not fully understood even by those designing algorithms. This poses problems for identifying fully meaningful consent from those whose data is being collected (see 'GDPR' chapter below) or whether we are dealing with manufactured consent. Indeed, while data protection regulation is well-documented, legal fortitude against data-driven discrimination is more nebulous. Privacy-by-design rules could be used to ensure data analytics tools are designed fairly, or an ombudsman could be specifically tasked to deal with data-driven decision making (Custers and Ursic 2018: 343). Seaver notes that it simply is not true that humans have no role in algorithms, and comments that 'if you cannot see a human in the loop, you just need to look for a bigger loop' (2018: 378).

1.4.2. People analytics

People analytics in human resources is defined as the use of digital tools based on big data sets or other data accumulation and aggregation, to predict, measure, report and analyse employee and potential employee performance; design workplaces; manage workforce talent; and to carry out a wide range of workplace operations. People analytics are operating at every step of the way in human resources, from recruitment and hiring practices using psychometric tests to digitalised interviews. Through applying a set of scientifically informed new applications, one company with Innovate UK funding called Arctic Shores, indicates that it can identify applicants' 'authentic behaviours' (Arctic Shores 2020), and thus help management to 'objectively distinguish between candidates on a wide range of traits' (ibid.).

There are several new products offering applicant tracking software which identifies and collates specific terms from CVs and used for performance management, via such cloud-based services as Microsoft's Delve and Rescue Time, which are software packages that monitor workers' specific activities and identify patterns; and a range of other innovations. Therefore, there are two new actors in the employment relationship in people analytics practices beyond the manager and the managed: 1) the software designers who set up the related programmes being introduced into human resources practices, and thus workplaces; and 2) more metaphorically, the machines and tools themselves, to which are attributed autonomous and 'artificial' intelligence, or automated intelligence, at interesting new levels, including predictive, prescriptive, assistive, collaborative and affective (Moore 2020a).

One IBM (2018) report claims that half of Chief Human Resources Officers anticipate and recognize the potential for technology in human resources surrounding operations and the acquisition and development of talent. A Deloitte report shows that 71 per cent of international companies consider people analytics a high priority for their organisations (Collins et al. 2017), because it should permit organisations to conduct 'real-time analytics at the point of need in the business process ... [and] allows for a deeper understanding of issues and actionable insights for the business' and deal with what has been called the 'people problem' (ibid.). 'Actionable insights' could be observed, for example, if a pattern in data indicates the rise in absences and changes in measured productivity in a workplace across workers or individual worker. A Chartered Institute for Personnel Development (CIPD) report (Houghton and Green 2018) refers to 'actionable insights' obtained from people analytics data that can be used to deal with what is referred to as people problems and risks, as quoted above. These practices can lead to significant stress for workers, particularly if they do not know what, nor why such data is being collected (Moore 2019) (see Worker Cameos chapter).

Cherry (2016) explores the risks of discrimination in people analytics where management's 'search for new pools of quantitative data are correlated with business and employment success' and data is used to 'make workplace decisions and to replace subjective decision-making by managers' (ibid.: 7). The use of big data gathered by various objective sources should provide possibilities to eliminate unconscious human bias that is linked to institutionalised racism and the ongoing gender pay gap that exists in most countries. If the practices that exist, however, are unfairly balanced, where e.g. a machine is trained to spot words that candidates use in applications and CVs, that are then used to determine candidates' eligibility for positions are the kinds of words demonstrating specific values or then realized to be used more commonly used by men, then the results will lead to more men bing hired over time. Where the number of men hired exceeds number of women, and the resultant dataset shows that the number of male employees is larger, then, the choice of text used for screening, which is a choice then that becomes a behaviour, the resultant data can be translated into recognisable institutional bias. Precisely in this way, the case that made recent mainstream news is whereby one AI tool used by Amazon for hiring purposes led to discriminatory outcomes, i.e. the text spotted by machinic processes led to the hire of more men than women (Dastin 2018). These technologies could even function to prevent resistance (Boewe and Schulten 2017).

What also arises in people analytics, or what should arise in terms of lines of questioning, is not only what is being counted, e.g. productive labour or other performance metrics, but what is *not* being counted. Whole arenas of activities contribute to the labour process, where preparatory work, affective labour, emotional labour, and domestic work are part of the social reproduction of entire labour forces, business structures, family and social lives and the surrounding norms upon which the stability of these forms are reliant. But this work is unpaid and under-acknowledged, and are often carried out by women and marginalised groups of workers (Moore 2018a).

Sánchez-Monedero et al. (2019) estimate that 98 per cent of Fortune 500 companies are currently using applicant tracking systems in their hiring processes, processes which includes sourcing, screening, interviewing and selection/rejection, where each stage is a form of automation with the intention to mitigate discrimination in automated hiring systems. The article argues that the legal bases for data collection and bias vary across countries. Software invented and developed in the US such as HireVue and Pymetrics therefore may not be eligible for usage in the UK nor across the EU. Dr Ian Brown[1] recommends the EU incentivise technical interoperability in systems produced by the largest companies, allowing smaller firms to compete with the near monopolies in the software and hardware industry where tracking and monitoring software is produced. Brown advises that, in order to address the problem of variable data law across countries, various components should be

[1] Interview with Ian Brown, an independent regulatory consultant, held by present author 25/07/20.

produced and manufactured by various companies, which can then be purchased modularly by a company to design a system that is oriented around a collectively agreed workplace problem. European businesses using North American technologies in particular must be cautious as product functionality may step outside of the parameters of what is permitted within European data protection law. The GDPR requires any non-EU company providing services within EU member states to abide by its rules on personal data processing, and the interoperability model Brown (2020) suggests will also help international companies to do so.

Designers should be made aware of the implications of usage of the technologies that they are creating and trained in this arena. The European Parliament's 2017 resolution on robotics and AI makes it clear that:

> …Asimov's Laws must be regarded as being directed at the designers, producers and operators of robots, including robots assigned with built-in autonomy and self-learning, since those laws cannot be converted into machine code. (European Parliament 2017)

Asimov's Laws, which this great science fiction author had proposed via a short story called 'Runaround' written in 1942 and appearing in the collection *I, Robot*, published in 1950, are that:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

These iconic phrases allude to the role of the human behind the design and development of the robots themselves, but the thinking and intention of engineers and developers working to create robots and machines behind the scenes are not divulged or addressed within these Laws. Indeed, it is often the case that designers of the software and algorithms as well as hardware and devices used for tracking and monitoring workers, do not have any background in ethics training based in social science, criminology, philosophy nor psychology, despite the range of different kinds of human practices made possible by the machines they create.

Sociometrics is another workplace tracking activity in people analytics, whereby a small device worn around the neck not only records workers' locations (normally in offices or other professional environments), but also records tones of voice and arm gestures as well as locations of clusters of people. Humanyze is leading in this field and talks about how the product can identify good practices for productivity through talent management (Humanyze 2020). The surveillance possibilities are obvious, particularly when data is collected over the course of time, and if datasets are used to feed into machine learning algorithms to make human resource decisions for e.g. promotion based on aggregate scores. Based on sociometrics data, if a boss wants to decide to give people who have talked to more people in a variety of locations throughout the day, higher scores, they could ask workers to give consent for their identities to be revealed, and then gain that data through looking at an individual's patterns of activity and movements around the office throughout the day over a period of time. While Humanyze's CEO claims that there is no way to identify the worker by the devices without asking (BBC World Service 2019), it would not be difficult to discern who workers are in companies fewer than 100, anyway, where data is cross-tabulated.

To be clear, people analytics is a highly attractive arena of work surveillance in human resources and can lead to some positive outcomes, but to avoid the margins of risk for workers, accountability must be established, given the serious implications of what can be done with data and how data can result in discriminatory practices. Now, the report turns to another arena of practices and tools in worker surveillance initiatives, where the physical and mental wellness of workers are becoming increasingly tracked and monitored.

1.4.3. Corporate wellness tracking

Many devices are marketed as providing self-improvement and empowerment in the arena of health and wellbeing for users, originally popularised in the 'quantified self' movement (Moore 2018c; Kent 2018; Ajana 2018), and now, we can even 'feel' our own data (Lupton 2017). Corporate wellness initiatives are increasingly tied to the usage of wellness-oriented devices (Till 2019; Moore 2018a, 2018c). As workers are increasingly expected to work anywhere and all of the time, to personalise and game the experience with a wellness focus, devices that both support and also track these behaviours, are becoming increasingly attractive. BP America was one of the first companies to offer step-tracking armbands as part of a voluntary company-wide initiative in health and well-being in 2013, and the investment in wearable devices in industrial and healthcare wearables, was expected to grow from USD 21 million in 2013 to USD 9.2 billion by 2020 (Nield 2014). More than 13 million wearable fitness tracking devices were predicted for incorporation into workplaces in the years between 2014–19 (ibid.). In 2016, an estimated 202 million wearable devices were distributed by employers as a part of various wellness programs (Edwards et al. 2018). As part of certain wellness programs, employers can get access to what is probably considered quite private personal information about their staff, such as if they have stopped taking birth control, whether or not they vote, and what drugs they take (Ajunwa et al. 2017). The global value of this industry reached USD 57.2 billion in 2019 (Grandview Research 2020).

Accelerometers, Bluetooth, triangulation algorithms and infrared sensors allow managers to monitor workers far beyond traditional hours logged by swipecards. Increasingly, 'many wellness programs now address things like emotional well-being, mental health and financial wellness' (Kohll 2016) and the benefits of improved productivity and employee wellbeing are continuously trumpeted. Self-tracking steps, sleep, heartrate and so on, are all part of a 'quantified self' movement originating in San Francisco in the mid 2000s that has inspired a now significant literature on technologically influenced corporate wellness initiatives which examine how the practices of tracking for wellness signify a social shift and penetrate other domains (Lupton 2012; 2013). Much biometric and other data related to employee wellness is collected via wearable devices, the introduction of which has been a growing trend in the last number of years. The 'quantified employee' (Bersin et al. 2016) is similar to a high performance athlete in a high pressure environment where technology is used to identifying peak performance times and to obtain rapid feedback. These trends are part of a rising 'surveillance society' (Lupton 2012) and 'surveillance capitalism' (Zuboff 2019).

In a case study by present author Moore (2018a, 2018b), funded by the British Academy/Leverhulme and entitled 'Agility, Work and the Quantified Self', a series of surveys and interviews was carried out with workers in a company in the Netherlands where a 'Quantified Workplace' (so-named by the company) experiment was being carried out. Workers were invited to collect data about the physical steps they took throughout the day, as well as their heartrates and sleep data (all taken from FitBit HeartRate armbands which the company gave to them); productivity scores based on RescueTime, which is a software that collects data on work activities such as 'composition', 'communication' and so on, based on screen time work; and data from a daily lifelog email where each participant was asked to rate their feelings of subjective stress and personally perceived productivity, over the course of 2015-2016.

The Quantified Workplace project took place before the GDPR was fully rolled out, so the 'meaningful consent' dimension was not as developed and challenged as it is now, but all workers Moore spoke expressed that they were mostly happy to take part in the project, at least at the beginning, not least because their experiences were meant to lead to the design of a new product. Workers were provided personalised dashboards, but data was also cross-analysed via a shared dashboard, which all participants, including management, could see, and thus they could compare one another's data. Ajunwa et al. discuss the significance of the use of shared dashboards (2017).

While it is plausible that there be other reasons for implementing shared dashboards, these are a proven way to create competition between workers and induce them to orientate themselves more attentively towards whatever metrics are being recorded and displayed on such dashboards (Levy 2015). Based on this data, management were able to identify specific periods of time with stress or joy or other emotions as linked to, for example, productivity and movement and 'billability' as the CEO of the company called it (Moore 2018a). Workers were at first, quite comfortable with their data being collected and viewable to colleagues and bosses, but by the end, they began to question why the data was being collected and for what purpose. In fact, the project saw a high rate of exodus, where more than ¾ of the project participants stopped wearing the armbands and tracking themselves by the end of the year the project ran.

Fitbit tracker devices have also been implemented by large companies in efforts to reduce their costs with insurance companies and to improve employees' health behaviours (Rosenblat et al. 2014). In one case, an employee wellness program allegedly involved employees having to tell of their sexual activity and weight, and if one refused to participate in the wellness program one would likely have to pay an extra $600 dollars a year for this health insurance (2014: 5-6). Like other aspects of employment relationships, while employees may have the choice to opt-in or not, in principle, in practice, companies may take a negative view of reluctant staff and so real pressure may be applied related to job security to opt-in. Such programs, and the laws to regulate them, are still in their infancy, and the more employees opt-in, the more likely it will be that such levels of surveillance will become normalised. Edwards et al. (2018) warn workers who are eager or open to joining specific data collection processes, that the data gathered by these technologies could, in the future, be used by the employer for unwanted and unforeseen purposes, in a case of function creep (Ball 2010: 92). Some video recording can also carry out lip-reading. This kind of function creep is also at a biopolitical level, where e.g. transcript data can be accumulated, based on an image.

BetterWorks is a software programme designed for workers, which 'blends aspects of social media, fitness tracking and video games' (Betterworks 2019) by obliging them to track their progress on a dashboard viewable by everyone in the company. Workers' progress is shown as a visualisation by a tree which can grow or shrivel. The company's website indicates that: 'technology should make everyone's lives easier, not harder. Betterworks merges with your existing workflow and reaches employees wherever they already spend their time' (ibid.). FitBit Health Solutions is another product that includes a smart watch and a smart scale, where the 'one solution for your whole population' in a way that will 'help drive meaningful engagement' by kitting out workers with self-tracking wellness tools and applications (FitBit Health Solutions 2019). Farr writes that 'companies have increasingly used a combination of carrots (free vacation days!) and sticks (higher premiums) to coerce employees into participating in health screenings and wellness programs' (Farr 2016).

Gathering data about workers' health and fitness is legally dubious, but many companies claim that they look only at aggregate data, making it difficult to identify workers. The GDPR clearly changes the game for privacy of workers and potentially gives companies access to data collected across the European Union, but the Health Insurance Portability and Accountability Act (HIPAA) does not cover non-insurance linked wellness programmes, so trust is increasinbly necessary. Christopher Till (2019) argues that corporate wellness programmes have the effect of capturing and controlling workers' attention and work habits, perhaps even more prominently than stabilising material health outcomes.

FitBit's market share was secured in 2015 due to its success with new corporate wellness packages (Whitney 2016) called 'Daily Activity Tracking Software'. This allows workers to work as normal in front of a computer terminal, but at the behest of a software programme that monitors interruptions to work, and records inactivity at the terminal, shows results that are allegedly automated and accurate. Software designers promise that tracking will help workers with productivity levels. They promise to help 'take control of your daily work time'. FitBit also sells tools to monitor activity,

timesheets, timekeeping, daily activity tracking, daily time tracking sheets, organisation helps, personal productivity amounts, productivity management, time reporting, and a tool to calculate overtime. Another company has been experimenting with a 'happiness metric' that measures employee's morale every two weeks, checks workers' motivation, and identifies team health based on 'regular pulse checks of the morale of their employees' (Power 2016) in a method that appears to resemble that of 'agile' (Moore 2018a).

Many applications now can identify calories burned, depending on activity and heartrate. A lens being developed by Google would measure blood glucose levels via the accumulation of tears from one's eyes. Tiny LED lights surrounding the lens would only become visible when glucose levels reach certain thresholds. Smart lenses would have the ability to take a reading per second, identifying information about changing blood glucose levels for users. Another rapidly growing research and development area is identifying and measuring emotions which is already being trialled in job interviews. One research team gathered information about the oxytocin levels of people watching commercials, to identify emotional resonance (Purdy et al. 2019). The study was seen to have the capacity to reveal what people 'really feel', which people often are not honest about. Indeed, emotional AI technologies are claimed to have the potential to identify emotional reactions 'in real time', through 'decoding facial expressions, analysing voice patterns, monitoring eye movements, and measuring neurological immersion levels' (ibid.).

However, there are clear potential problems with using such identifiers in workplaces. Imagine if management judgement of workers' negative feelings were to have a negative impact on career progression. Emotions change quickly, are usually considered in psychological categories outside 'logic' and 'rationality', and cultural ways of expressing these vary. So, they are much more difficult to measure with the standard scientific measures. Emotions manifest themselves physically differently. Some people sweat when they are stressed. Others may find their mouths dry out. Some people's heart rates increase due to anxiety and others', reduce.

Before too long it will be possible for employers to quite literally track workers' blood, sweat and tears and to use this data to feed algorithms for fully automated decision-making purposes, whether in human resource decision-making or corporate wellness initiatives, or a mixture of both. This area of research may produce the most concern for the new surveillance, where even the biological and the affective must be quantified, as present author Moore argues, not for fairness or salary purposes, but to predict worker collapse (2018c) i.e. to see at what point a worker will not be able to come to work anymore. The problem arises when, rather than looking at the working conditions within which the worker works, data is trusted to give accurate information about a person and any red flags along the way for a worker's route to collapse are ignored by an institution.

Now we turn to look at a relatively new arena of monitoring that has implications for worker tracking, that of genetics.

1.4.4. Genetics tracking

One response to the collection of data in the corporate wellness sphere with the purposes of protection for workers' data is the use of the Genetic Information Non-discrimination Act (GINA). While less successful in its intended field of genetic medical testing, this Act could provide a blueprint for a future statute protecting workers' privacy against employers' data practices. In its first decade of execution in the medical and health insurance fields, the broad implications of big data for privacy were discussed but not resolved. However, Areheart and Roberts (2019) see GINA as an approach that was intended to address public fears about genetic discrimination 'before it started'. This blueprint prevents health insurance companies from requesting genetic data and using it in their rating decisions, but it also classifies family medical history as protected genetic information and prohibits employers (and other employment-related entities) from discriminating on the basis of genetic information. GINA's principles could provide a blueprint for employee-

privacy protection, with the potential to protect workers' data (particularly in terms of reproductive health and disability) where technology could render other anti-discrimination laws and statutes seemingly obsolete.

Big data accumulation compounds surveillance issues by virtue of the scale and depth of these practices. The ability to analyse trends from big data accumulations that might not be conventionally accessible is troubling, and inferences may be illegitimately drawn from them. Indeed, GINA's wellness-programme provisions allow employers to use employee health data, but the conditions in which they can do so are substantially restricted (requiring voluntary written authorization from employees and with data received only in aggregate terms). In terms of future protections, two key aspects of a GINA-inspired model could be increasingly useful for protecting workers' health related data:

> 1) protecting recognised antidiscrimination classes (by prohibiting the request, requirement or purchase of information pertaining to a protected status),
>
> 2) protecting sensitive information (i.e. protecting attributes and categories beyond the scope of established protected characteristics).

Indeed, legislators could limit employer access to either particular types of data, data that does not pertain to employment, or even to sources of potentially sensitive data. The GINA model thus potentially 'strikes a reasonable balance between antidiscrimination and efficiency'.

The next chapter identifies the use of wearable and handheld technologies in new surveillance workspaces.

1.4.5. Wristbands and handheld devices

Wearable self-tracking and handheld devices are increasingly seen in workplaces. GPS, radio frequency identification (RFID) and now such features like haptic sensors are likely to replace the use of clipboards and pencils for warehouse workers. Amazon Technologies, Inc. made a patent request in 2017 for a new type of wristband for Amazon workers in fulfilment centres. While Amazon workers already gain orders via arm-worn devices, the product would offer a new function that guides workers throughout warehouses by buzzing against the wearer's skin and directing the wearer to the correct location. A haptic feedback mechanism tells the worker whether an identified inventory bin is correct or incorrect, whether an inventory item is recognised or unrecognised by the management module and is used to '[guide] the user to a designated inventory bin associated with the inventory system task'. The wristband contains a motion detection unit, which can be used by the worker to signal the accomplishment of a task by moving the wrist band in a predetermined manner. This should save time for workers. However, this could constitute the next stage of surveillance techniques to ensure management know at all times where workers are and what they are doing. Amazon has been criticised extensively, such as by a writer for the New Yorker magazine, where stories from warehouse workers who were injured and then fired were reported (Duhigg 2019). The article shows that over the counter painkillers were freely available in 'vending' machines. Warehouse workers raced against quotas to keep themselves in very low paid and dangerous and difficult menial work. Another interpretation would be that the wristbands provide Amazon's managers with new workplace surveillance capabilities that can identify which workers are wasting time, fidgeting or dilly-dallying.

The patent application text for such Amazon devices describes the product as follows:

> Inventory management systems and related methods employ radio frequency based tracking of a worker's hands to monitor performance of inventory tasks. An inventory management system includes inventory bins, a user – wearable unit configured to be worn in proximity to a user' s hand, fixed RF antennas configured to transmit at least one RF

> interrogation signal and receive at least one RF response signal, a RF transceiver operatively coupled with the fixed RF antennas, and a management module operatively coupled with the RF transceiver . The user - wearable unit includes an RF transceiver configured to transmit RF response signals in response to reception of the at least one RF interrogation signal. The management module is configured to process signals generated by the RF transceiver to track locations of the user - wearable unit and identify an inventory bin based on proximity of the user - wearable unit to the identified inventory bin to monitor performance of an inventory system task. (Brady 2018)

Another patent application, also by Amazon Technologies, Inc., is for an 'ultrasonic tracking' device to track workers' hands and 'monitor performance of assigned tasks' (Brady 2018). The system could also track workers' hands in relation to the location of inventory bins so that tasks could be allocated properly. The patent suggests 'a suitable communication means' (indicator LEDs and/or haptic feedback) could be used to provide instructions and directions to workers. The system can be configured to emit further information such as timestamps, duration of use, faults, etc. including the implementation of WiFi or infra-red transmission (Cohn 2017). Workers in some grocery superstores in the UK are allotted handset computers to gather items for shopping delivery orders. Devices assign and provide location information about items but workers report that the devices track productivity constantly, and do not adjust for size of the items nor size in the trolley required, and that they cannot turn off the devices even when taking a toilet break or helping a customer (Plan C 2017).

Motorola has been leading in handheld and worn worker devices since the beginning of the 2000s. The MC3000 handheld scanner, designed for 'maximum user productivity' is intended to be used in warehousing, loading docks and on delivery routes. It is available in a number of interface configurations, including touch display, image capture, barcode scanner, and voice/audio feedback capability. Real-time processing enables fast performance and mobility, and the device can be interoperated with PCs, web services, servers and other devices. It weighs between 379g and 555g, and its ergonomic design is intended to reduce fatigue for higher productivity (Motorola 2009).

Another Motorola device, the WT4000 is designed to 'enhance worker efficiency and productivity' with a wrist-mounted, hands-free design which can be used in conjunction with a finger-mounted 'ring scanner' (see Gent 2018) or a back-of-the-hand which means workers can handle objects while interacting with the computer. In addition to its graphic display, the WT4000 can be used in conjunction with a headset to enable voice picking. Workers receive instant feedback for incorrect items, and a fast WLAN connection which means data can be processed in real-time to improve decision-making and reduce errors. The ergonomic design empowers warehouse and package handling workers to achieve new levels of efficiency, productivity and accuracy (Motorola 2008).

Smart glasses are another kind of worn tracking and monitoring device, which are used for training and assistive purposes, and we will look at these in the next chapter because augmented reality is being trialled alongside these items in work environments.

1.4.6. Augmented reality (AR) and smart glasses

Augmented reality (AR) technology is now being experimented with in logistics via hardware platforms in handheld devices; stationary AR systems; spatial augmented reality (SAR) systems (e.g. 3D projection); head-mounted displays (HMDs); smart glasses; and smart lenses (which are still theoretical). If used in warehousing operations, AR technology could reduce costs by optimising picking processes, which would allow pick lists to be displayed within a worker's field of vision, while barcode scanners track worker's locations and actions. DHL claimed in 2014 that these systems had the capability to 'bridge any barriers with migrant workers'. In transportation optimisation, AR could be used for checks in delivery/pick-up processes, regulation compliance (e.g. import/export), and could allow face recognition software to identify authorised receivers. Finally, AR could potentially

remove the need for skilled workers in assembly and repair roles, where AR systems could train and supervise less-skilled workers and ensure quality control in real-time. The main 'technical and societal challenges' include 'battery life, high investment cost, network performance issues, privacy, and public acceptance' (Glockner et. al. 2014).

There is a US patent application made by Amazon Technologies, Inc. for a wearable augmented reality user interface which presents workers with a display of changing information based on location and inventory data. The patent drawings show a high number of location identifiers via barcodes and QR codes which populate the interface of a wearer's field of vision, such as on inventory stacks, shelves, stock items, the floor and so on. Based on the location data captured by the interface, envisioned as goggles or glasses configured with a barcode scanner, image capture, RFID scanner, NFC scanner and/or Bluetooth, inter alia, the AR display would provide workers with directions (configured to avoid the locations of other users), instructions, locative cues (e.g. rings circling a correct item), and confirmation of the successful task completion. The wearable 'can also be equipped with one or more sensors that can detect movement, acceleration, orientation, and other aspects of the position of the device'. The system transmits information about tasks performed by the worker across a given period of time, including map data and item data (Madan et al. 2018).

Surveillance aspects of these devices include the possibility to collect very detailed information that could show workers' whereabouts constantly throughout the working day. The VR goggles would track orientation data, pitch, yaw and accelerometer data 'which could translate to things like walking speed and their exact location' (Gizmodo, cited in SupplyChainDigest 2018). One line in the patent text refers to a possible nudge system whereby the device would prompt a worker to get back to work (ibid.). One Freedom of Information (FOI) request targeted information about how Amazon data was used for human resource decisions and led to the receipt of documents detailing the scale of some full-time Amazon associates who were fired for inefficiency. Documents calculated more than 10 per cent of Amazon's staff annually in one fulfilment centre were sacked for failing to reach productivity targets. The documents say productivity warnings and even terminations are generated automatically by the system rather than by supervisors, though Amazon clarifies supervisors can override the process. The system also tracks 'time off task'. Despite these signs, Amazon says its productivity goals are set objectively (Lecher 2019).

The Verge gained, also by an FOI request, a letter from Amazon's attorney to the National Labour Relations Board's attorney in the USA. NLRB had claimed on behalf of an Amazon worker that the worker had been fired for making complaints about unreasonable productivity requirements, rather than for their failure to meet production quotas. Amazon's attorney claimed in the letter that 'the criteria for receiving a production related notice is entirely objective – the production system generates all production related warning and termination notices automatically with no input from supervisors'. The attorney clarifies, however, that errors in 'policy application' can be corrected by human resources. Amazon's 'proprietary productivity metric for measuring and weighting productivity of each associate' is referred to in the letter, which, in the US case, is based on several weeks' of performance data from across North America and 'evaluated quarterly to make modifications as necessary'. Modifications to productivity rates can be suggested by managers, but they are enacted by teams outside any given facility. The letter details the case of the employee, who was forced to undergo a mandatory re-train, in which they demonstrated an inefficient box-packing method. The letter states that between August 2017 and September 2018, 'Amazon has terminated hundreds of employees at the BWI2 facility alone…for failure to meet productivity rates'. Attached to the letter is a redacted appendix detailing each termination (Carey 2018).

The next chapter looks at the use of platforms in the monitoring and surveillance of workers.

1.4.7. Platforms

The platform service industry has grown significantly since the first Amazon Mechanical Turks worker (soon called a 'Turker' or 'crowdworker') logged into the relevant platform and looked for work or bid for a job in 2005, and the first Uber drove a passenger in 2011. The so-called 'gig economy', a term first coined by Tina Brown in 2009 in the *Daily Beast*, is portrayed by a growing number of workers she had noticed, who appeared to be chasing:

> …a bunch of free-floating projects, consultancies and part-time bits and pieces while they transacted in a digital marketplace. (Brown 2009)

Jobs that are obtained as piecework via platforms and their surrounding economy has attracted significant attention due to the nature of the low-quality contracts available to workers who are part of this labour market and the working conditions they endure. Gig work is obtained via online applications (apps) and websites such as Uber, Upwork, or Amazon Mechanical Turks. The work can be performed *online*, where work is obtained as well as carried out on computers, like design work, translation and programming; or *offline*, where 'gigs' are obtained online, but carried out offline. Such work includes taxi driving, food and parcel delivery and cleaning work and other domestic services with low level maintenance. There is a lot of scholarly research now which looks at online gig work in a global labour market (e.g. Berg 2016; Brawley and Pury 2016; Graham et al. 2017a, Graham et al 2017b; Hitlin 2016). In both online and offline gig work, extensive data is collected about workers which ultimately decides whether or not they have access to paid work.

The definition of 'platform' is not universally agreed. It can be understood as a technical matter, where 'digital platforms are complicated mixtures of software, hardware, operations, and networks ... [which] provide a set of shared techniques, technologies, and interfaces to a broad set of users' (Kenney and Zysman 2016: 64). Srnicek talks about the infrastructure within which platforms operate, from a political economy purview, as 'a powerful new type of firm' (Srnicek 2017: 42), where data is almost a new type of raw material. Online platforms exist within a market in and of itself, where platforms are seen as 'enabling parties to contact one another for the purposes of some economic transaction' (Moore and Joyce 2020, referring to Codagnone et al. 2016). Moore and Joyce suggest that platforms should be understood within a more flexible definition which acknowledges the employment relationship and the relations of production that are inherent to operations within a new form of 'platform managerialism' (Moore and Joyce 2020). Platforms are mediators for the economic activity they facilitate, where the new form of technology is itself a kind of regulator (Donovan et al. 2016: 4). Many platform firms are very aggressive and seek to regulate their surroundings rather than be regulated by local laws. This is possible principally because any person, any time, can log on to the platform and begin to use it to find work, without knowledge or understanding of the legal parameters within which they should be operating, whether tied to the types of contracts that workers should hold, or the way that data should be processed and can be used, often behind the scenes, to manage workers.

The process of gaining and sustaining online and offline gig work both includes algorithms, location tracking and performance measures and systems that involve extensive aggregate customer feedback. Indeed, gig workers are reliant on good feedback ratings data just to gain more work. However, passengers and clients can behave in unfair ways, leading to unfair rankings which explicitly reduce people's ability to gain work (Berg 2016; Gandini 2018). The reputation economy is very important, and workers must have good profiles that are designed themselves which should help in the long searches for work using e.g. Mechanical Turks. Berg and De Stefano (2017) report that gig workers 'averaged 18 minutes looking for work for every hour working'. Tranches of feedback data are used to judge workers' performance and even lead to workers being removed from the system or 'deactivated', and thus not able to work. There is a kind of outsourcing of performance management functions to members of the public, via instantly accessible technologies, which happens instead of appraisals of trained managers working under equalities

management systems (Rosenblat and Stark 2016).Therefore, a surveillance loop is created, where workers are constantly watched, not just by the platform itself (and data fed back to companies) but also by clients. Aggregate data is used by clients to make decisions about who to select for work, especially for more skilled work as designing and translation work. Indeed, automated surveillance in platform work is given 'intelligence' features with its AI augmented dimensions, those being selective, predictive and prescriptive intelligences (Moore 2020a) with regard to algorithmic client-matching and reputation determination.

In the article 'Limitless Worker Surveillance', Ajunwa, Crawford and Schultz (2017) discuss the online platform Upwork's in-built monitoring system. Upwork is a service where clients look for freelancers to do specific chunks of work for them, in web, software and mobile development, data science and analytics, customer service, admin support, and a range of categories listed on the website, where people post their CVs and gain work. While workers work, Upwork's system 'takes random snapshots of workers' [freelancers'] computer screens six times an hour, records keystrokes and mouse clicks and takes optional Web cam photos of freelancers at work' (Ajunwa et al. 2017: 747). This allows clients to check contractors' work at a very granular level of surveillance.

Briziarelli and Armano (2020) and Gandini (2018) show that digitalised work occurs in less definable spaces. This allows for exploitation, such as unreasonable surveillance of workers' activities, to occur. In gig work, time and space take new forms and efficiencies achieved in accelerated forms (Wajcman 2015) and digitalised management methods can be identified outside of the perceived black box of obfuscation (Moore and Joyce 2020; see Pasquale 2015). Data generated about workers by the platforms used in gig work is treated as an arbiter and judge with more legitimacy than other qualitative judgements. If a taxi driver using the Uber platform is fatigued and makes errors, there is no appraisal available for him/her and so the driver cannot express the need for less working hours and better working conditions. Unions have emerged and workers have begun to organise against what are often very poor working conditions (Waters and Woodcock 2017), where algorithmic management becomes less like 'management' as traditionally understood and looks increasingly like a form of top-down surveillance with fewer and fewer avenues for negotiation and workers' rights.

Delivery gig workers are held accountable for their speed, number of deliveries per hour and customer rankings, in an intensified environment of workplace surveillance. In Harper's magazine a driver explains how new digitalised tools work as a 'mental whip', noting that 'people get intimidated and work faster' (The Week 2015). Drivers and riders are at risk of deactivation from the app if their customer rankings are not high enough or they do not meet other requirements. This results in occupational safety and health (OSH) risks, including blatant unfair treatment, stress and even fear (Moore 2018b). Silberman and Johnston have published a good ETUI guide to using the GDPR to protect platform workers (2020) that focusses on the beneficial possibilities for workers' subject access request for data.

1.4.8. Ergonomics and Virtual Reality

Present author Moore arranged to visit the technology research center entitled 'Laboratory for Ergonomics and Virtual Reality' at the University of Applied Sciences Koblenz Faculty of Mathematics and Technology (11/09/2019) for the research activities of the current report. At this laboratory, researchers carry out experiments with technology, where they have fabricated work stations and carried out human engagement activities. Their work is designed to produce useful empirical research as well as to identify possible products and to observe surrounding arising issues, from a scientific and socio-technical perspective. Dr Michael Bretschneider-Hagemes, who is the chief trade union officer of the Office of the Social Partners (Sozialpartnerbüro Arbeitnehmer), Kommission Arbeitscschutz and Normung (KAN), and doctoral researcher Patricia de Paiva Lareiro of Weizenbaum Institute, also attended.

The group met with research centre leads, Dr Daniel Friemert and Prof Dr Ulrich Hartmann, and spoke to the researchers in their labs. Discussions were based on the various technological projects they are running, which are directly as well as indirectly linked to possible workplace uses. There are three laboratories in this Centre: the Laboratory for Biomechanics, Ergonomics and Virtual Reality; Exoskeletons and Musculoskeletal stress; and Software engineering and Data Science. In the first lab, the focus is on ergonomics. Here, three projects are underway. In the first, a 3-year project financed by the BGHW has been carried out, in cooperation with the logistics department of a hardware tool manufacturer. The effects of monocular data glasses on OSH in a simulated warehouse have been investigated. The aim of the project was to prepare a recommendation for action for the use of data glasses at workplaces in the areas of trade, logistics, service and assembly.

From the OSH perspective, Dr Michael Bretschneider-Hagemes[2] indicated that he sees a huge amount of stress and mental strain in terms of firstly, being observed all the time without knowing related reasons and usage by a company or organisation; and secondly, because of a shift in the power structure and the relationship to the employer as a disadvantage for employees and works councils. The employers knows your work in terms of scales and metrics better than the worker, but even then, scales and metrics do not show the full picture. This trade union expert indicated that they only show what is explicitly decided from employers side for benchmarking employees. As a result, there is an ongoing intensification of work enabled by the collection of these data, which itself makes implicit knowledge explicit. That is the reason why Bretschneider-Hagemes and others speak about a new wave of (digitalised) Taylorism/scientific management.

In the Applied Sciences laboratory, researchers built a life-sized fabrication of a warehouse picking station. The structure feeds objects into a carousel that spits them into a locator were workers select and distribute them into appropriate chapters of this picking station, to their left and right. Previously, a screen above workers' heads would instruct the workers where to place each object. The introduction of data glasses to the experiment was intended to better the working conditions and especially the ergonomics of workers who would not have to move their heads upward and downwards as frequently as when using a screen.

Within the laboratory based study where monocular data glasses were used, of the 29 test persons, 9 were from the logistics industry. In the study, movement patterns and the workers' speeds were tested, comparing the traditional workplace set up with a centered monitor which provided the picking instructions and the data glasses. While there was no improvement regarding workers' efficiency, their movement speed decreased, which could be a sign of a selection of fewer unnecessary movements. For the experiment, motion capturing suits were used. Within the scope of field and laboratory studies, subjective and objective types of stress at real and reconstructed workplaces are recorded. Stress is evaluated according to ergonomic aspects with the aid of standardised questionnaires and appropriate measurement technology. The workplace implications are that the reduction of unnecessary movements could reduce stress and improve the economic quality of the workplace. Workers report eye strain and headaches after long term use e.g. in two years, if monocular glasses are worn for the whole shift, every workday.

The surveillance implications of the first project in this lab are as follows: the practices of using data glasses as mentioned above, can permit intensified analysis of which worker is carrying out work at what point; and this surveillance aids in generating data about accuracy of work carried out. The physical movements linked to ergonomics are also then more intensively viewable to management in ways that perhaps Taylor and the Gilbreths could have only imagined.

[2] Interview conducted by Moore with Michael Bretschneider-Hagemes 12/07/20, trade union officer of the Office of the Social Partners (Sozialpartnerbüro Arbeitnehmer), KAN - Commission for Occupational Health and Safety and Standardization, Germany.

Daniel Friemert indicated during the lab visits, that the perception of data glasses in worker interviews is often negative at first. The key problems are technical, for example, the glasses get hot. Workers also do not like the other parts of the compound system. After a long time using data glasses, people complained of seeing spots and numbers after taking the glasses off. After several hours of work with HoloLens's augmented reality with gestures, users sat in their resting rooms and tried, in vain, to close the windows with gestures. Some workers who used them for 2 years complained about eye strain and headaches.

In the second laboratory, the influence of exoskeletons on musculoskeletal stress in overhead work, such as in factories where workers screw parts into the bottom chapters of cars, is being investigated. Researcher Mirko Kaufmann, in cooperation with an airplane assembler, was running this project, which focusses on motion analysis and the simulation of joint movements to investigate the influence of exoskeletons on task performance and health issues (e.g. blood flow). The motivation for the use of exoskeletons for workers is predicted staff cost reductions, based on a reduction of medical absences. It is also argued that assistance system would be a cheaper alternative to fully automating the overhead tasks. The workplace implications involve such things as dealing with reports of numbness in the fingers, however no data on long term medical consequences yet exists. Surveillance implications are again linked to identifying and making judgements about physical movements of workers.

The third project, run by researcher Christopher Braun, has to do with participation-based training models for safety officers, training that should result in the prevention of falls with the help of virtual reality. The project's financial backing was provided by the BGN (Berufsgenossenschaft Nahrungsmittel und Gastgewerbe), and its training tool has been positioned to raise awareness of the safety hazards of trips and falls. The workplace implications are that the short term use of VR applications for training purposes could benefit active learning processes. Surveillance implications are in a similar domain to those of data glasses for workers, and activities will be carried out by trainers and managers.

2. The employment relationship in the new surveillance workplace/space

In the new surveillance workplace; or work*space* as mentioned already, it is not always the manager nor owner of a company who is doing the monitoring, but the situation can be more complex and is affected by broader trends and processes. Machines have clearly advanced in capabilities and come to be used in an increasing range of the work we do, both manual and cognitive (Moore et al. 2018a). In fact, the majority of the tools used for workplace monitoring are now digital (Ajunwa et al. 2017). This has led to what Graham and Wood depicted to be a 'step change in power, intensity and scope' (2003: 228) in digital surveillance.

Traditional understandings of surveillance, where the parts played by the one who observes, and the one who is under observation, are now outdated. Once, one knew who is searching, and who is sought. In the workplace, in a similar way, it was once more obvious who was being watched, and by whom, e.g. in scientific management where the manual worker was watched by the mentally superior manager. That hierarchical employment relationship is now less prominent and binary roles are not as clear since the digital mediation of surveillance is seemingly ubiquitous. Identification, profiling and analytics are generated via algorithmic means, rather than via the previous methods of clandestine human and analogue investigations.

The 'employment relationship' contains two aspects, the first being 'market relations' and the second, 'managerial relations'. Market relations have to do with the price paid for work and surrounding benefits such as pensions. Managerial relations involve how tasks are defined, who defines tasks, how the manager 'gets' the worker to do the work and what will happen if the work is not done or the quality is low (Edwards 2003: 11). Research in industrial relations traditionally focusses on these arenas. Here, the report looks at how the employment relationship at these two levels is becoming reformed because of the introduction of new technologies.

In that light, this chapter looks at what the introduction of new technologies means for workers and for managers. The increasingly ambivalent nature of the employment relationship must be viewed through the following lens: one's mobility, where people's physical workplaces are digitalised and therefore increasingly variable; the new types of flexibilised contracts where workers have less job security; and the volatility of the labour market, where local and global economic crises are commonplace. All professions and types of work in a variety of skills groups see some kind of monitoring and tracking and so concerns around the fragmentation of privacy and data protection probably permeate all employment relationships in all workspaces. Here, we look at some of the issues arising within and for the employment relationship in a variety of new surveillance workplaces/spaces.

2.1. New privacy concerns in service work

The service sector has over time featured very high levels of workplace surveillance. Ball (2014) identifies houses of gambling, call centres and logistics workplaces as the frontrunners, largely due to low union density in such contexts and thus less active resistance to the technology being implemented. However, most service workers, whether academic, engineering, civil service, or design, will probably have to link with their employer's mainframe technology, and by this fact their activities become more open to being monitored (Bélanger and Thuderoz 2010). Service work sees a range of new surveillance techniques that are significant for the employment relationship.

The location, speed and direction of workers is being monitored, but now other types of data related to movements are also accessible, including physiological measures (like heart rate and number of steps taken in a given time). Transportation and logistics industries are prime candidates for

tracking, and truck drivers and warehouse operators, already discussed, have targeted. Now, technology is also being implemented in office contexts, in the financial sector, where companies try to prevent e.g. insider trading by monitoring employees' lines of communication (The Guardian 2017). Tracking is seen in hospitals, where nurses are reported to be equipped with badges that track how regularly they wash their hands (Ajunwa et al. 2017: 110). Body heat and movement levels are monitored, as well as physical gestures and tone of voice - now accessible via RFID and which are incorporated into workers' chairs and desks in newspaper companies and others (Moore et al. 2018b). Movement tracking technology has existed for a number of years, and the most up to date versions have a far greater scope and precision than past iterations (Moore et al. 2018b). One concrete example is the case of Tesco, where management analysed the data from movement monitoring software, and determined to reduce its full-time staff by 18 per cent (Wilson 2013).

Technologies can also be used to monitor and set limits to employees' access to different rooms in offices where services like design and architecture work occur. Some Smartcard and other ID systems used to enter and exit rooms and buildings are now based on facial or iris recognition, as well as scans of fingerprints, where increasingly personal, granular data is collected and maintained by the employer (Schumacher 2010). Sociometric Solutions developed ID badges that feature a built-in microphone, accelerometer and location tracker (see People Analytics chapter). Sewell and Barker (2006) tell of a Japanese case where monitoring software was used to track and find family members who had dementia. The software was subsequently introduced into police departments and sales teams to track the location of any employee, whether they were standing up, running, walking, or if they had fallen over.

So, for security reasons and otherwise, the employment relationship is no longer so neatly structured around what workers can expect concerning privacy. Read the Worker Cameos chapter in this report for examples of the challenges to privacy in the employment relationship. Privacy relations are certainly changing in the service industry employment relationship as more and more types of data are becoming visible.

2.2. Coercion and criminalisation in call centres

An important example showing how workplace/space surveillance practices across various countries is Poster's case study of call centre workers in India (Poster 2018). Often, North American client companies outsource call centre roles to the Global South where labour law is weaker than other areas of the world and wages are much lower. Poster's research demonstrates that there is very intensive surveillance used throughout contact centre buildings, and there are almost-militarised checkpoints and barriers limiting entry to certain parts of the building. Supervisors and team leaders in the Global South have fewer autonomy or possibilities to challenge these environments and are, Poster shows, treated differently from their colleagues of equivalent rank in the Global North, where 'clients in global call centres treat managers just like workers—as potential criminals. The result is that even the highest-level staff are under surveillance by clients' (Poster 2018: 167).

In terms of organisational design and practices, data collection has tended to be operationalised via more coercive supervisory styles than collaborative, in call and contact centres. Ajunwa et al. draw attention to the lack of legal barriers in some locations to management teams from accessing collected raw data, even though the company claims they do not record conversations or provide the raw data (Ajunwa et al. 2017). With light protections, even 'private' conversations between colleagues could potentially be listened in on by bosses. But even where there are legal protections, findings in the present report show that one call centre worker in a European country discovered even private conversations with colleagues between calls were being recorded and commented on by management (see Worker Cameo chapter, Call Centre Frontline Worker). Methods focus on problems, or foreseen threats in the call and contact centre environment, and do not genuinely work

toward empowerment or career development of employees, even though more participatory management styles are promised (Ball & Margulis 2011: 119; Smith et al. 1981). Once a manager labels a worker as a poor performer, based on monitored data collected about them, it can be unlikely that they change their mind about them, and extra effort will be put into further monitoring work practices and productivity, rather than taking more developmental steps (Ball and Margulis 2011). Bronowicka et al. (2020) have produced a more recent report on call centre surveillance in Germany and Poland which identifies worker representatives' frustration with ongoing blocks to access of information about data collection as well as struggles to find avenues for union presence in bargaining around call centre workers' rights.

2.3. Trust issues emerging

Surveillance can decrease trust in the employment relationship (Ball 2010; Rosengren and Ottosson 2016), where the introduction of surveillance practices can signal a lack of trust in staff. The violation of perceived trust interestingly, can have the negative side effect of reinforcing the supposed deviant behaviour the surveillance was implemented to counteract or prevent and can certainly lead workers to not trust their managers. It has been established that if monitoring is inappropriately designed or implemented, it can significant raise workers' stress levels (Nebeker 1987), as can monitoring systems that lead to disciplining, rather than training or development (Nebeker and Tatum 1993). The felt presence of an unseen audience can also lead to those under surveillance being apprehensive or feeling inhibited (Ariss et al. 2002). Using experimental methods, Aiello and Svec (1993) found that when comparing the completion of tasks while being monitored vs unmonitored, participants who were unmonitored performed more strongly than those being observed (whether in-person or electronically).

The suspicion of the misuse of time, called 'time-theft' and 'loafing', is central to the rationale behind the growing phenomenon of the new surveillance workplace/space, although this is not the only activity staff are suspected of. There are similarities between contemporary concerns of time-thievery and elements of the Taylorist era a century ago. Indeed, 'similar moralistic comments as those espoused by Taylor arise, but with an added criminalising emphasis' (Stevens and Lavin 2007: 41). This happens in the context of broader and historical negative images and reputations associated with wage labour, with the figure of the worker being a 'despised character' (Rosengren and Ottosson 2016: 183). Perhaps it is the case that the tried-and-trusted method of emphasizing trust within the employment relationship could be a far more effective tool than non-transparent monitoring, for improving employee performance (Ariss et al. 2002).

The marketing of new surveillance technologies also gives us an insight into the logic behind them and the types of dangers the manufacturers see as important to employers as well as the supposed protections that are provided for workers (see Sánchez-Monedero et al. 2019), revealing the ambivalence the new tracking technologies pose for the employment relationship and workers' experiences. The Abacus group communicates to potential users that their product can 'tell you which members of the team are idling away their time' and 'prevent fraudulent and abusive use of your phones and networks' (Stevens and Lavin 2007). The CEO of Awareness Technologies compares the relationship between employer and employee, with that of a parent and their child, saying, 'If you are a parent and you have a teenage son or daughter coming home late and not doing their homework you might wonder what they are doing. It's the same as employees' (The Guardian 2017). 'Worksmart' software monitors workers by taking periodical photos and screenshots of them and framing the technology as a tool for employee betterment. One worker responded to the software by saying: 'OK, I'm being monitored, but if the company is paying for my time how does it matter if it's recording what I'm doing? It's only for my betterment' (The Guardian 2017).

2.3.1. Function creep

Ball (2014) gives three primary reasons why companies decide to digitally surveille workers. The first reason is to ensure productivity and keep track of resources used by staff; secondly, to protect company and trade secrets; and thirdly, to collect evidence in case it would be needed in a legal dispute. Some organisations also cite the general goals of 'efficiency' and 'innovation' as grounds for implementing employee monitoring. But all of these goals translate into large data sets and it is tempting to identify reasons to use the data for more reasons than are originally set out, leading to a practice called function creep (Ball 2010: 92). This emerges in surveillance systems where the scope and extent of monitoring expands without the consent or consultation from workers about the other uses of that data. Function creep is forbidden by the GDPR via purpose limitation discussed in Art. 5(1)(b), which indicates that personal data must be:

> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

The misuse of data collected to document workers' tasks through function creep can also lead to mis-prioritisation of specific tasks, which is known to reduce the levels of trust within organisations. Likewise, the creativity of workers is reduced if they know that their communication, behaviour and output, are being closely watched with opaque possibilities for data usage. Sometimes the implied significance of different aspects of tasks can be unintentionally (mis)communicated to employees, e.g., the relative importance of quantity over quality; and of course, information that a company or organisation holds about its employees can sometimes end up in the hands of unauthorised third parties (Ball 2010).

2.3.2. Time tracking and discipline

One standard goal of worker monitoring is to track and record the complete working day of staff, which, via more advanced technological solutions, also enables organisations to statistically compute and analyse how their employees spend not just working time, but potentially, all other moments of their days as well (Stevens and Lavin 2007). Time stamped collected data enables management and supervising teams to make various calculations, and develop systems and organisational practices built around time regulation. However, in case of potential future conflicts with an employee, this detailed record of their time (mis)use could nefariously be utilised by management in disciplinary proceedings. Levy (2015) also discusses management's desire for their staff's daily and hourly behaviour and activity to be rendered visible, and ideally measurable and available for analysis. This analysis and the actions and changes that follow it can be unpredictable, and do not necessarily follow whatever the initial logic was for implementing monitoring and data collection systems.

2.3.3. Competition amongst workers

Data produces the possibility for statistical generation and analysis, which can feed into work barometers and standards. Indeed, standards and metrics can be used as the material for creating comparisons and competition between colleagues, teams, company offices, and entire regions. The data from such comparisons can then be drawn upon by management to make comparisons across groupings and create a gamified and competitive environment, as well as to make decisions about which workers are performing best/worst and even used in future disputes with employees. In this way, statistics and their perceived-to-be reliable knowledge that emerge can be fed back into the labour process in ways that increase management's possibilities for workplace/space control. One empirical example is in the management of a truck-driving company, where information and

statistics which were collected about drivers were re-oriented to develop social pressures and competition amongst drivers as well as to introduce new pressures on drivers' *families*. Bonus cheques, based on collected driver scorecard data, were posted out in the names of the drivers' wives, whereby 'wives are expected to create pressure for their husbands to continue meeting the company's organisational performance benchmarks' (Levy 2015: 171).

On the topic of the relative importance of monitoring for productivity and how much it should be prioritised within a healthy business, the managing director of Accenture's talent and organisational practices cautioned managers that 'If you have to check up on employees all the time, then you probably have bigger issues than just productivity' (The Economist 2009). Even under earlier iterations of electronic monitoring, workers have likened their experience to being whipped 'not in our bodies, but in our minds', and always being apprehensive and inhibited due to the awareness of an 'unseen audience' watching over them (Fairweather 1999). Ariss et al. quote the case of someone who worked in data services, whose life had become intolerable due to their screen flashing all the time while they worked, inferring the message: 'You're not working as fast as the person next to you' (2002: 23-24).

Since employee surveillance systems must necessarily find their place in the broader context and history of an organisation as well as the surrounding labour processes, cultures and business processing trends, they can have different impacts and become embedded in different ways. They can play a role in negotiations regarding working conditions, and at times be appropriated and used by worker groups (Ball 2010). Those tasked with doing the monitoring may also choose to utilise a piece of technology in different ways, sometimes purposefully ignoring certain aspects or manipulating for their own ends (Bain and Taylor 2002; Ball 2010). It is common for employees being monitored to try to evade the gaze of these technologies, or resist in other 'idiocultural' ways including the creation informal social meanings and ordering (Zirkle and Staples 2005). Such attempts and practices of workers aimed at circumventing electronic surveillance are obviously limited in their potential, and cannot replace traditional forms of resistance such as trade unions or the utilisation of labour law (Ball 2010). Allen (et al. 2007) found that employees often face a risk if they try to challenge organisational norms where monitoring of employees and a disregard for worker privacy are institutionalised facets: 'Employees usually do not come forward and complain about or question the company's rule. If they did, they could lose their job' (Allen et al. 2007: 191). Regardless of the creative ways employees may find to resist, such attempts will remain within hierarchical employment structures.

The potential for these intensive surveillance practices to cause harm to workers is well-documented at this stage. Levels of self-esteem, confidence, anxiety, stress, and paranoia have all been shown triggered by monitoring, as well as the likelihood of developing nerve disorders and carpel tunnel syndrome increased (Schumacher 2010). Kizza and Ssanyu (2005) list stress, repetitive strain injury, alienation, and decreases in creativity, self-esteem and communication as potential outcomes of increased employee monitoring, while Henderson et al. show electronic monitoring can raise workers' blood pressure (1998). Workplace surveillance can contribute to creating an atmosphere of fear, where those being monitored are made afraid of losing their job, and can also have a negative impact on trust levels within an organisation or team (Sarpong and Rees 2014; Alder 2001; Mujtaba 2003). It is not only the very reality of being monitored that can cause stress in employees, but also the lack of control that they have in the systems watching them (Varca 2006).

While monitoring and metric systems can be effective ways to increase productivity, they can also cause people to overwork, and be the cause of injury to themselves. Kaplan (2015) mentions a monitoring system implemented by the delivery company UPS which saw employees ignore and disobey safety rules in attempts to reach their given targets. This disregard for safety ended up putting their and others' lives at risk. In another example related to professional drivers, the electronic surveillance implemented in Karen Levy's case study resulted in truck drivers skipping

breaks that were legally mandated and being discouraged from listening to their own bodies as the guide for when to sleep (2015).

Tales about the intensity of the labour process and levels of monitoring in Amazon's warehouses have been heard widely around the world in recent years, and warehouse workers have gone on strike against such practices on numerous occasions in 2018 and 2019 (GMB 2018; BBC 2019; The Guardian 2018; Huffington Post 2019). As part of an effort by Amazon to maximise efficiency, workers have their movement speed and location in the warehouse tracked to see how fast they load and unload products, and if they do not work fast enough and fall short of certain targets they will lose their jobs (Rosenblat et al. 2014). It has been reported that the intensity of these monitoring systems and the pressure they put on workers to meet their targets have led to staff having to work while in agony, being prevented from being able to go to the bathroom to urinate, a heavily pregnant woman being forced to stand, and ambulances being called to the warehouses (GMB 2018).

The following chapter outlines the genealogy of privacy and data protection legal activities over time, where the introduction of new technologies into society and increasingly into the workplace and space have raised concerns for the European Union and beyond.

3. Privacy and data protection legal instruments and cases

In 1981, early advances in the computer industry increased awareness of privacy issues and induced the introduction of set of legal criteria with regard to automatic processing of personal data called the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No. 108, was launched in Strasbourg on the 28th of January 1981 and after five ratifications rolled out in 1985. The potential of this Convention was not realised, however, due to the poor and inconsistent ratification of the Convention by signatories. However, in 1989, things changed. The unification of East and West Germany increased demand for privacy in Germany due to the release of data the Stasi had collected from millions of people during the GDR. West Germany had already established significant privacy law since 1977 whilst surveillance was underway at very high levels in the East. This historically significant event in Germany in 1989 alerted the European Commission to consider the extent of variations in local law and the implications for the idealised possibilities for the free flow of data across the EU. A multilevel framework with uniform national responsibilities was not available, and it quickly became clear that something needed to be done.

3.1. The Data Protection Directive 95/46/EC

The Data Protection Directive 95/46/EC of the European Parliament and of the Council of the European Union was arranged in the 1990s, with emphasis placed on the point that national laws should protect people's right to privacy, as required by the European Court of Human Rights (ECtHR). Formally the Convention for the Protection of Human Rights and Fundamental Freedoms, originally drafted in 1950, the European Convention on Human Rights (ECHR) was firmly reflected in the Data Protection Directive 95/46/EC (Directive 95/46/EC 1995). In particular, it was made clear that ECHR Article (Art.) 8 should be built into the national context within the guidelines and wider principles of EU law.

ECHR Art. 8 calls for the 'Right to respect for private and family life, home and correspondence'. The core of this Article is that:

> Everyone has the right to respect for his private life and family life, his home and his correspondence. There shall be no interference by a public authority concerning the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (ECtHR 2020: 7)

ECHR Art. 8 is extremely important for privacy and data protection rights and is repeatedly sourced in case law, seen in the country case studies chapter in the current report. Art. 8 has extensive scope for worker protections with regards to data and privacy, where the sphere of private life is detailed with regards to physical, psychological and moral integrity, within areas from mental illness to issues concerning burial, sexual orientation, sexual life and business activities. Privacy is then outlined in the Article's text, where data protection, right to access personal information, protection of individual reputation and issues of defamation are relevant for workers and relevant relations. Family life, Home, and Correspondence are then further embellished in the text. A chapter of Art. 8 outlines, of relevance for the workplace/space context, 'Correspondence of private individuals, professionals and companies', after which it comments that:

> Contracting States have to be granted 'a wide margin of appreciation' as regards the legal framework for regulating the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. That said, the State's discretion is not unlimited. (ECtHR 2020: 105)

The Data Protection Directive 95/46/EC was written to ensure the rights enshrined within the ECHR including Art. 8, are incorporated. This Directive outlined people's protection regarding the processing of personal data and the free movement of such data, where personal data is defined as 'any information relating to an identified or identifiable natural person' (Art. 2(a)). Member States were asked to prohibit processing of personal data concerning, for example, 'health or sex life' (Art. 8(1)). The Directive was implemented 24 October 1995.

So, the Data Protection Directive 95/46/EC was the first binding international instrument to protect people against abuses in collecting and processing personal data and to regulate the flow of personal data across borders. It was very strict on sensitive data, where information about people's race, health, sexual life, religion and criminal records must not be processed without legal safeguards. The Directive was updated a number of times and has now been repealed and replaced by the GDPR.

Internationally, data protection regulation is rooted in the OECD's Privacy Principles, which are part of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which were developed in the 1970s and fully introduced in the 1980s. These Principles were also incorporated into the 1985 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data referred to above, and are closely linked to the European Commission Data Protection Directive 95/46/EC now updated by the GDPR (Custers and Ursic 2018: 330).

3.2. Article 29 Working Party

An independent EU advisory body called the Article 29 Working Party whose full name was 'The Working Party on the Protection of Individuals with regard to the Processing of Personal Data',

Which became known as the Art. 29 Working Party (already indicated previously in the current report as 'Art. 29 WP'), was established in 1996 (and is now replaced by the European Data Protection Board, acronym EDPB, which has endorsed Art. 29 WP works). The membership included the Data Protection Authority from each EU Member State and representatives from the European Data Protection Supervisor and European Commission. Its purpose was outlined in Art. 29 of the 95/46/EC Data Protection Directive, where the Party was expected to:

- Provide expert advice to the States regarding data protection.
- Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland.
- Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data.
- Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community. (European Commission nd)

A 'Working document on the surveillance and the monitoring of electronic communications in the workplace' (Art. 29 WP 2002), also often just called 'the working document', was drawn up, which emphasised an important point, which is that monitoring and surveillance which merely serves the employer's interests is *not enough* to fully justify intrusions into workers' privacy. Indeed, the Art. 29 WP was set up to evaluate the implications and surrounding issues of data protection specifically for workers and employers around issues of how electronic communications at work and surveillance and monitoring practices should be handled. The Party emphasised that fundamental data protection principles must be demonstrated in any monitoring practice in the workplace, which are: transparency, legitimacy, proportionality, accuracy, finality, security, and staff awareness. It key principles are legal grounds, transparency and automated decisions (Art. 29 WP 2017: 5).

The Art. 29 WP suggested that monitoring should demonstrate:

> A proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers. (Art. 29 WP 2017: 23)

In 1997, Alder and Tompkins had already reported that there were approximately 26 million electronically monitored workers. Their findings demonstrated that dialogue with workers during the design and implementation phases of tracking, restrictions over monitoring to performance-related activity that can be used for positive feedback, and in general, two-way communication and involving employees in the practices of technological implementation is more likely to result in positive results for a company than more coercive practices and monitoring that could also operate outside specifically defined work-related parameters. So the use of 'concertive control' potentially violates 'organisational justice' (Alder and Tompkins 1997). While computerised monitoring provides more possibilities for providing feedback, the question also could be posed: how much feedback is too much, and how can it be constructed appropriately to ensure improved worker performance (Alder 2007)?

The first decade of the 2000s saw the internet and computation in the office become increasingly part of business processing systems. Many employers were interested, as computers were increasingly present at work, in limiting workers' personal use of the Internet, but limiting its use was quickly realised as a very 'demanding challenge for the law', and in 2010, Lugaresi noted the lack of 'persuasive, exhaustive and shared legal responses yet' (2010: 263). Lugaresi sees the internet as an increasing extension of private life itself, so the use of the internet is not an outlandish expectation, but if an employer has not created a privacy policy, workers do not have the automatic right to use it. The level of privacy granted to workers rests with the discretion of employers, but their power and policy contents must be intentional and restricted.

Lugaresi argues that is hard to maintain there is a right to a personal use of the internet. Even if unavoidable, it is not an employer's responsibility to provide for such a service. In fact, 'the DPWP emphasised "that it is up to the company to decide if workers are allowed to use the internet for personal reasons and the extent to which this is permissible"' (DPWP 2002: 24 cited in Lugaresi, 2010: 165-166). There must be a balance, knowing that in the end the decision is taken by employers, as it is a part of their right to run their business, and that in doing so, they may adopt a blanket ban on personal use of the internet. Workers who are provided with computers, email addresses and online access and by the employer, have no inherent right as such (according to Lugaresi 2010), to personal use of the internet. Now, the internet is almost a basic utility, and it is very difficult to perform many activities in general everyday life, without it, so it is increasingly difficult to forbid workers from using any form of the internet in the workplace.

European and American law differ, whereby US law gives quite a lot more surveillance power to employers than European. As said, usage of the internet had become part of nearly all workers' private lives, and that area of life inevitably had begun to enter business processing operations and private lives alike. In Europe, the EDPB updated the Art. 29 WP with the rollout of the GDPR in May 2018. In the final year of its existence in 2017, the Art. 29 WP published Opinion 2/2017 on Data Processing at Work (Art. 29 WP 2017). Opinions do not hold as much weight as other soft law instruments in European law, but nonetheless, its focus on nine specific scenarios where modern technology has increased the ability of the employer to monitor employees is illuminating. The Opinion is clear that workers have the right to private zones at work, stating that 'it should be ensured that employees can designate certain private spaces to which the employer may not gain access unless under exceptional circumstances'. The Opinion also notes that the right to these private zones cannot be excluded by any 'agreement' between the parties. In providing a framework for employers and employees, the Opinion leans heavily towards avoiding breaches of privacy through forward planning via the 'protection by design' principle. Three elements should form the core for employment policies: transparency, proportionality and data minimisation.

3.3. The General Data Protection Regulation (GDPR)

The GDPR was originally formulated to deal with the new technologies on the market designed to collect new data in new ways, about workers and consumers. We will focus on the implications it has for workers here.

The 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016' was introduced to deal with the topics of the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This was tied to the repeal of Directive 95/46/EC and the introduction of the GDPR. The Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, was then linked to the repeal of Council Framework Decision 2008/977/JHA (Eur-Lex 2019). In 2016, the EU adopted the GDPR, which replaced the 1995 Data Protection Directive. In 2018 as of May, the GDPR was recognised as law across the EU. Member States were given two years (2016 - 2018) to work to ensure that it is fully implementable in their countries. National legislation in the European Economic Area (EEA) is required to ensure adherence to the GDPR and all other actors in countries hoping to do business with European companies are also liable.

The GDPR is a highly significant advancement in data and privacy history, and has been widely perceived as a game-changer across the EU and the world. The Irish Data Protection Commission, for example, has celebrated the introduction of the GDPR, which replaces the Data Protection Directive 95/46/EC, noting that:

> [The GDPR] significantly changes data protection law in Europe, strengthening the rights of individuals and increasing the obligations on organisations. (Irish Data Protection Commission 2019)

This statement captures the essence of the Regulation. The key advantages for workers are that it contains more protections for them than the Data Protection Directive 95/46/EC in a number of ways. Revisions permit data transfers to non-party states but only when personal data is protected; require data minimisation and proportionality; provide rights in the area of automated decision-making, where algorithmic transparency is recommended; and require prompt notification of data breaches. Furthermore, the GDPR requires stricter enforcement mechanisms than the Directive, where each country must have national supervisory authorities in place who will require compliance. In fact, significant fines are associated with failing to keep to GDPR requirements, where fines for infringements are up to a maximum of €20 million (about £18 million) or four per cent of annual global turnover, whichever is greater (see GDPR Breaches).

The provisions of the GDPR indicate that the rights around automated profiling and decision-making apply to *all* automated individual decision-making and profiling. Automated individual decision-making is where an actor would set out to make a decision solely by automated means without any human involvement, based on profiling, which means:

> …any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (GDPR Art. 4.4.)

Profiling can indeed be a part of automated decision-making processes. The UK ICO outlines these principles and instruction for companies as follows:

> Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
>
> You can only carry out this type of decision-making where the decision is:
>
> necessary for the entry into or performance of a contract; or
>
> authorised by Union or Member state law applicable to the Controller; or
>
> based on the individual's explicit consent. You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
>
> give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that your systems are working as intended. (ICO 2019)

Data Controllers play a very important role in ensuring GDPR policy is met. Indeed, Art. 24 outlines the responsibilities of the Controller, which are to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary' (Eur-Lex 2019). Art. 25 extends these responsibilities with a discussion of 'data protection by design and default', whereby the Controller is responsible for implementing appropriate technical and organisation measures like pseudonymisation, measures that secure data minimisation efficiently and integrate safeguards and to protection data subjects' rights (Eur-Lex 2019). The Controller is also responsible for informing data subjects about the receipt of personal data from other sources and to communicate to the data subject their rights with regards to this data (Art. 14).

Art. 6 of the GDPR, 'Lawfulness of Processing', indicates that data processing is lawful 'only if and to the extent that at least one of the following applies' (GDPR Art. 6):

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. 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;
3. processing is necessary for compliance with a legal obligation to which the Controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
6. 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.

In other words, a Data Controller must carefully consider whether or not at least one of these criteria can be defended as a legal reason for data collection and processing. Clearly any consideration in this area is complicated by the variable dynamics, organizational history and other aspect of all work environments. Nonetheless, one or more criteria should be selected and communicated to workers clearly in cases where data processing is carried out.

The rights of the data subject are outlined in Art. 12, where transparent information must be relayed to the person whose data is being collected. The Controller is responsible for facilitating a data subject's exercise of their rights (Art. 12: 1-2) and responsible to respond to a data subject's requests for information within one month. Information must be given free of charge. The data minimisation principle is very important, because, as the current report details, digitalisation and data exchanges have evolved significantly (Ogriseg 2017 R8) allowing for significantly larger datasets to be assembled than in previous times. In essence, Data Controllers should not gather and collect more data than they need for a specific human resource solution, with agreement from unions and worker representative groups.

Alison Powell has identified the principle of 'viability' when exploring modalities for data collection and its correspondent protection. Dr Powell's work on smart cities and as part of the Horizon 2020 VIRT-EU project has addressed some issues that touch on workplace practices and information systems. She suggests to strive for 'minimum viable datafication' in system design, which includes efforts to:

1. Look holistically at an organisation, focussing on adherence to principles for data protection but further extending frameworks for ways to think thru ethical consequences for what is being built.
2. Be clear what problem is being solved and identify the minimal viable amount of data necessary to solve it.
3. Connect social values and data protection in considering a data collection system.
4. See workers collectively as individually in data collection and aggregation.
5. Identify responsibilities and their connections within the process of data collection and processing systems, continuously addressing workplace ethics.

These principles are intended to allow an organisation to consider the viability of plans in a broader ethical context than the immediate intention of system optimization.

Data subjects should not suffer a loss of privacy and data security just because there are possibilities to advance optimization of a system. Art. 32, which focussed on the security of processing personal data, emphasises that 'the Controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate' (Art. 32):

> (a) the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Ibid.)

Art. 14 states that the Data Controller is him or herself responsible for informing data subjects about the collection of their personal data from sources and about their rights with regards to the data surrounding access, rectification, erasure, restriction of processing, data portability, notification of explanation in the event of automated decision-making. Data subjects need notification if the Controller intends to disclose data to third parties. This should relieve the worker herself from having to continuously check whether due diligence is followed with regard to the GDPR regulations (ibid.).

Of great significance for the processes of decision-making now within the remit of the use of numeration and various metrics, Chapter 4 of the GDPR outlines the 'Right to object and automated individual decision-making'. Art. 22, called 'Automated individual decision-making, including profiling', indicates that:

> 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The foundations for the Regulation, listed in the first chapters of the document also make it quite clear that:

> (71): The data subject has the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significant affects him or her, such as… e-recruiting practices without any human intervention. Such processing includes profiling that consists of any form of automated processing of personal data evaluating the personal aspects of a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work… reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

It is worth noting here that employment contracts do not always cohere with legal principles and it has been increasingly the case that workers are forced into a position of having to query processes, because they have not been informed of either what data is being collected nor why, nor how it is stored, processed and used. Workers are almost always already in a vulnerable position in the employment relationship, and it is an injustice that workers have been continuously expected to ensure basic enforcement and protections of their rights. Some EU judgements have emerged as the GDPR was rolled out, such as the Bărbulescu case outlined below, which indicates that no employment contract should have precedence or authority over existing laws and regulations protecting workers' dignity and human rights. While this is the case, a number of data and privacy principles themselves abide in mutual dissonance (see Tensions in Legal Principles).

The GPDR contains a few specific guidelines to implement and affect the rules within it. In the early phases, each country was expected to devise their own national set of rules to safeguard workers' data and rights. However, the EDPB, which replaced the Art. 29 WP, is providing guidelines and recommendations for best practice at various points, which should lead to consistent application of the GPDR (Art. 70 par. 1(e), Regulation 2016/679/EU, cited in Ogriseg 2017: 4).

Another headline area in this field is the introduction of AI into worker surveillance. The recent rediscovery of possible uses of AI has excited many professionals who are interested in identifying how AI can enhance work and business. The employment relationship, productivity, talent management and so on, are all increasingly impacted directly by AI.

3.4. Guidelines on Artificial Intelligence and Data Protection

AI augmented tools and applications have been increasingly part of the uptake of electronic and mechanised new surveillance workspace experimentation in factories, warehouses, offices and work which occurs on the streets and in homes alike (Moore 2019). AI is touted as a superior solution in decision-making and optimization, and even celebrated as holding civilization potentials, where public spending in the billions for research and development AI outpaces many other types of technology funding, and competition in this arena has been fierce, where the US tends to lead, and China and Israel are in close second (Delponte 2018). China claims it will use AI to boost GDP by 2030 by 26 per cent, and North America aims for a 14.5 per cent boost (PwC 2018).

AI is often linked to automation and potential job losses but it is more suitably described as an augmentation tool for data collection and usage that may or may not advance those possibilities, rather than a stand-alone entity, or in ways that confuse precise definitions. The Internet of Things, automation and digitalsation in general terms sometimes overlap with discussions of AI itself, but it is vital to adhere to definitional precision. The mission to automate human intelligence is probably the most accurate and a better way to think about AI in the workplace. Computation machines are expected to have the intelligent capability to make predictions, to be prescriptive and make decisions, as well as to have sufficient intelligence in the assistive, collaborative and affective domains to become a recognisable and useful actor in the employment relationship and in the new workplaces and spaces of today (Moore 2020a).

The European Commission's definition of AI in its 2020 White Paper reads that it is a 'collection of technologies that combine data, algorithms and computing power. Advances in computing and the increasing availability of data are therefore key drivers of the current upsurge of AI' (European Commission 2020). The European Commission's definition as provided in the 2018 Communication is also useful, as it indicates that AI 'refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals' (European Commission 2018). *European Artificial Intelligence leadership, the path for an integrated vision*, a 2018 report for the European Parliament's Committee on Industry, Research and Energy, defines AI as a 'cover term for techniques associated with data analysis and pattern recognition' (Delponte 2018: 11). That report differentiates AI from other digital technologies in that 'AI are set to learn from their environments in order to take autonomous decisions' (ibid.). These definitions identify the scope and context within which AI is understood to have the potential to affect workspaces as well as take into account the sometimes incorrect blanket use of the term. Indeed, AI machines and systems are seen to demonstrate competences which are increasingly similar to human decision-making and prediction. AI augmented tools and applications that are intended to improve human resources and tracking of productivity, attendance, and even health data for workers, are often seen to perform much faster and more accurately than humans and thus, even of managers (see chapter on People Analytics).

The backbone of AI development relies upon swathes of semi- and unskilled data workers in both the Global North and South who carry out digital 'dirty work' (Roberts 2016) in social media and data services. These workers, who Moore calls 'AI trainers' and smart workers (see Moore 2020b), include content moderators, who curate content for social media platforms such as Facebook and other news and video services; and data service workers, who work with data via annotation and natural language process training for such products as Amazon's chatbot Alexa. This is the most difficult and psychosocially debilitating work in the digital industries today. While news reports have demonstrated that their work is damaging psychologically, traumatic and difficult (Newton 2019a, 2019b), what has been sorely overlooked is that the main, and very lucrative, asset that these workers provides is identification data of specific images or types of text, which are then used to create huge databases, which are necessary used to train machines for AI. Therefore, AI trainers' work adds significant value to social media platforms and smart devices, and contributes to the development of AI. Moore talks about the invisibilised affective labour that these workers carry out to self-manage the worst elements of such work (Moore *forthcoming*).

AI systems already automate some perceived human work such as the affective labour that Alexa speakers provide. In 2018, Price Waterhouse Coopers indicated that AI is likely to create as many jobs as it is predicted to eliminate (PwC 2018). We have to ask, however, *what kinds* of jobs are created, as these could include the very traumatic work and highly surveilled and monitored work of content moderators or the tedious work of data service workers referred to above. Consultancies' predictions have been published as well as several governmental, regional and international organisations' high level reports which predict the significant impact of AI on economies and societies, including the United States of America (White House Office of Science and Technology

2018); the United Kingdom's Department for Business, Energy and Industrial Strategy and Department for Digital, Culture, Media and Sport (2018); the International Labour Organisation of the United Nations (Ernst, Merola, Samaan 2018); and the European Union (European Commission 2018).

As a response to the uptake and hype around AI and work, as well as usage in consumer spheres, the Consultative Committee of Convention 108 released Guidelines on Artificial Intelligence and Data Protection in early 2019 (Directorate General of Human Rights and Rule of Law 2019). These guidelines give insight into the 2018 GDPR, confirming that decision-making powers with AI-produced data must be curbed and human rights upheld. Overall, the recent shift in data protection regulation in the EU puts much more emphasis on people's access to, and control of data; examines the rights to withdraw consent for data to be collected and used; and emphasises where the data must be secured. Such regulations apply to consumer and worker data alike. These are huge steps.

Also in 2019, the OECD published 'Recommendations of the Council on Artificial Intelligence' which states that AI will be a good opportunity for 'augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, sustainable development and well-being' (OECD 2019). These positive statements are encouraging and throw some hope into the mix, but as Aloisi and Gramano (2019) point out, AI may also engender or push forward 'authoritative attitudes… perpetuate bias promote discrimination, and exacerbate inequality, thus paving the way to social unrest and political turmoil'. Sewell (2005) warned of the ways in which nudges and penalties, introduced by AI-augmented incentivization schemes, create tense working situations. Tucker (2019) cautioned that AI influenced ranking systems and metrics can be 'manipulated and repurposed to infer unspecified characteristics or to predict unknown behaviours' (discussed in Aloisi and Gramano 2019: 119).

The European Parliament's 2017 resolution on robotics and AI acknowledges that the:

> …development of robotics and AI may result in a large part of the work now done by humans being taken over by robots without fully replenishing the lost jobs, so raising concerns about the future of employment, the viability of social welfare and security systems and the continued lag in pension contributions, if the current basis of taxation is maintained, creating the potential for increased inequality in the distribution of wealth and influence, while, for the preservation of social cohesion and prosperity, the likelihood of levying tax on the work performed by a robot or a fee for using and maintaining a robot should be examined in the context of funding the support and retraining of unemployed workers whose jobs have been reduced or eliminated. (European Parliament 2017)

This is highly insightful given the links made between the development of robotics and AI and the workforce and the 'viability of social welfare and security systems' to deal with the developments, even in 2017. The recommendations are highly important e.g. robot taxation and retraining for workers.

Hendrickx looks at whether the GDPR could be used to protect workers from the worst implementation of AI into workplaces that could result in automation. The three main rights that can protect data subjects where AI is operating, are:

- The right not to be subject to it;
- The right to be informed about it;
- The right to have a human interface. (Hendrikx 2019: 177)

De Stefano refers to the cover of one of the editions of the New Yorker magazine which shows humanoid robots giving handouts to a human beggar on the street (De Stefano 2019: 15). If history goes in the way that many pundits predict, AI will lead to a near-elimination of the need for human as producer.

3.5. The International Labour Office Protection of Workers' Personal Data Code of Practice

The International Labour Office (ILO) published the Protection of Workers' Personal Data Code of Practice in 1997, which is perhaps the most insightful soft law document of its time on data practices, many of these Principles reflect the current GDPR.

5. General Principles

5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.

5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

5.4. Personal data collected in connection with technical or organisational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.

5.5. Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.

5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance.

5.7. Employers should regularly assess their data processing practices:

(a) to reduce as far as possible the kind and amount of personal data collected; and

(b) to improve ways of protecting the privacy of workers.

5.8. Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.

5.9. Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code.

5.10. The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation.

5.11. Employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code.

> 5.12. All persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality consistent with the performance of their duties and the principles in this code.
>
> 5.13. Workers may not waive their privacy rights.

Principle 5.5, distinctly reflects the GDPR's Art. 22, which protects the 'right not to be subject to a decision based solely on automated processing' which is almost word for word from this Code. The ILO's' Code of Practice warns against function creep (5.2.) and elegantly discredits electronic monitoring and performance evaluation and automated processing (5.4. – 5.6.). Principle 5.10. emphasises the risks for data-based discrimination, which are now well documented (Ajunwa 2020; O'Neill 2016; Sánchez-Monedero et al. 2019). The GDPR Art. 13 Par. 2 details fair and *transparent* processing of data and workers' rights to detailed explanations of all automated processes that impact them, reflecting the ILO's Code in Principle 5.8. More than 20 years after the ILO emphasised these rights, the GDPR and other regulation updates today reflect these important guidelines. The emphasis on the role of worker representative groups is crucial. Workers and employers, the Code emphasises, 'should *cooperate* in protecting personal data and in developing policies on *workers' privacy* consistent with the principles in this code (5.11.)'. The emphasis on worker representation requires much more attention in the contemporary continuation in data rights debates and policy formulation.

3.6. Bărbulescu vs Romania

There are a number of data protection misconduct cases and privacy breaches that demonstrate where parties have been held to account for collecting data inappropriately, using it for incorrect reasons or otherwise falling outside the law. The one which stands out the most, having significant implications for the future of data and privacy protection regulation and policy, is Bărbulescu vs Romania. In 2007, an employee named Mr Bogdan Mihai Bărbulescu was accused of using a business Yahoo Messenger service to write messages to his fiancée and his brother, rather than exclusively using it to speak to clients about sales. When asked, Mr Bărbulescu indicated in writing that he was using the account only for business reasons. Resulting from this, management invited the employee to a meeting during which they showed him detailed transcripts of his exchanges. Bărbulescu's employment was terminated.

Mr Bărbulescu first made a formal complaint to the county courts in Romania, saying that the Romanian Constitution and criminal Code had been violated. The complaint was dismissed, because the Court ruled the worker had been informed of the regulations and had used company property for personal communications anyway. The judgement noted that:

> The employer's right to monitor their employees' use of the company's computers in the workplace falls within the broad scope of the right to check the manner in which professional tasks are complete… Some of the reasons that make the employer's checks necessary are the possibilities that through use of the Internet employees could damage the company's IT systems, or engage in illicit activities in the company's name, or reveal the company's commercial secrets. (European Court of Human Rights 2018)

Bărbulescu, however, appealed the decision, saying that his right to a private life and correspondence, guaranteed within the ECHR's Art. 8, had been violated, and also that he had not been permitted to call witnesses. The Romanian Court of Appeal dismissed the appeal in 2008, indicating that:

> In view of the fact that the employer has the right and the obligation to ensure the functioning of the company and, to this end, [the right] to check the manner in which its employees complete their professional tasks, and of the fact that [the employer] holds the

> disciplinary power of which it can legitimately dispose and which [entitled it] to monitorand to transcribe the communications on Yahoo Messenger that the employee denied having had for personal purposes, after having been, together with his other colleagues, warned against using the company's resources for personal purposes, it cannot be held that the violation of his correspondence (violarea secretului corespondenței) was not the only manner to achieve this legitimate aim and that the proper balance between the need to protect his private life and the right of the employer to supervise the functioning of its business was not struck. (Ibid.)

One of the judges in the case was partially dissenting to the decisions made, and in accordance with Art. 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, Judge Pinto de Albuquerque's views are annexed within the judgment text, arguing that there must be a balance between the employer's right to surveillance and workers' rights:

> Even where there exist suspicions of cyberslacking, diversion of the employer's IT resources for personal purposes, damage to the employer's IT systems, involvement in illicit activities or disclosure of the employer's trade secrets, the employer's right to interfere with the employee's communications is not unrestricted. Given that in modern societies Internet communication is a privileged form of expression, including of private information, strict limits apply to an employer's surveillance of Internet usage by employees during their worktime and, even more strictly, outside their working hours, be that communication conducted through their own computer facilities or those provided by the employer. (Ibid.)

The story did not end at that stage, however. Mr Bărbulescu was not satisfied with this judgement and finally took his case to the European Court of Human Rights, stating the Romanian courts were not protecting his right to a private life and correspondence ensured by ECHR Art. 8. The European Courts decided, at first, that it was not a breach and that the investigations were balanced. However, the Grand Chamber of the European Court of Human Rights reversed the decision later, holding that the balance was not appropriate. The Judge stated that 'an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary'. This is a welcome about-turn, but clearly some issues remain. While workers are seen to have a 'reasonable expectation of privacy' more frequently at work, the issues of the right to a private life are more vulnerable and appear to be more open for interpretation and compromise (ECtHR 2016; Jervis 2018).

Smith and Tabak (2009) draw some conclusions for practice regarding e-mail monitoring and.

There is a discussion of justifications for employers' e-mail monitoring and an analysis of case law, web-based private emails, and international implications of e-mail monitoring. The justifications for monitoring are: protecting the firm for liability risks, protecting company assets, and ensuring job performance. Electronic monitoring can be in the organisational structure as well as seen in management's desire for control as well as emerge from a desire to cut costs and monitor levels of productivity.

3.7. Arias vs Intermex Wire Transfer

In California in 2015, a sales executive named Myrna Arias sued her employer after being fired from her job for deleting the Xora job-management app which included GPS location tracking from her work phone. The application did not switch off even when logging off and meant that workers were tracked 24 hours a day, 7 days a week. The fired employee likened the software to having to wear a prisoner's ankle bracelet (Ajunwa et al. 2017: 105). The employee's boss had allegedly been bragging that he could see how fast she was driving her car, even while off-duty. Arias set out to sue the

employer. Her attorney indicated that the app allowed 'bosses to see every move the employees made throughout the day' (Kravets 2015). The case was settled out of court.

3.8. López Ribalda and Others vs Spain

In the case of López Ribalda and Others v Spain, workers in a store had been filmed by a number of video cameras, after management discovered discrepancies between stock and sales figures. Management informed workers that they would be under video surveillance, but did not reveal how many would be installed, nor the precise locations of cameras. In that judgment, in which the appellant relied on in its application, the ECtHR, stated that the measure taken by the employer (installation of surveillance cameras in a supermarket) was not proportional, linking two facts: on the one hand, non-compliance with the Art. 5 of the Organic Law of Data Protection, by failing to inform workers of the installation of hidden cameras; and, on the other hand, the indiscriminate nature of the recordings, which affected all the workers working in the boxes, lasted for weeks, and covered the entire working day. That is to say, no matter how heavy an employer's suspicions, the ECHR does not legitimise unlimited recording without informing workers in advance.

The ECtHR's judgment considered that the installation of CCTV directly affected the private life of all workers in the store, since 'the conduct of a person in his place of work, which cannot escape being to be obliged, under the employment contract', to perform work there. However, in October 2019, the ECtHR did not adhere to these views and finally made the judgement that the company's actions did *not violate* Art.s 6 and 8 of the ECHR.

3.9. GDPR breaches

As indicated, the GDPR holds more weight than previous data protection legislation, where, now, a company or organisation can be fined up to €20 million or four per cent of annual global turnover (whichever is greater) in cases of non-compliance. There have already been several GPDR breaches in appropriate protection and processing of worker data. In August, the Italian Data Protection Authority (Garante) fined Cavuato S.R.L. €10,000 for gaining access to personal data of a prior employee, including browser history, from a work computer. Garante fined Mape S.p.A. €15,000 for having an insufficient legal basis for data processing, whereby a company left the e-mail account of a data subject active and automatically forwarded incoming emails but did not provide adequate information. The Spanish Data Protection Authority fined Barcelona Airport Security Guard Association (AVSAB) for violating Art. 5(1), whereby a member of the committee was using WhatsApp to send messages to private phones which contained personal data about workers. This violates the confidentially principles that should be kept by a data controller as well as by other subjects in the data processing field.

The Dutch Supervision Authority fined one organisation 725,000 for violating Art. 5 and Art. 8 €725,000 for requiring staff to scan their fingerprints to record attendance. However, the Authority indicated that the organisation should not rely on the 'exceptions to the processing of this special category of personal data'. The company could not 'provide any evidence that the employees had given their consent to this data processing' (GDPR Enforcement Tracker 2020). These are only a few of the relevant cases that have happened only in the second year of this full enforcement era of this increasingly important Regulation.

4. Tensions in legal principles

A number of principles apply to the right to a private life and to protections around how workers' data is collected and used. This chapter looks at some of the tensions across principles and indicates where there may be difficulties in implementation of, for example, the GDPR today.

4.1. Inviolability vs power of command

The principle of the inviolability of the worker's right to a private life and private communication have been portrayed in law to grate against the principle of an employers' almost sacred private property and to maintain a managerial power of command (Reinhard 2002). However, some countries' constitutions explicitly protect workers' privacy as an inviolable right, such as the Spanish. The German constitution has no specific rules, but protection is inferred from other principles such as the right to personality. British law has no constitution, but rights are taken from other avenues (see country case studies).

Data processing about workers may function to protect employers' private property, but this does not merit *all* processing, and indeed, criminal law has to play a role if cases are brought which demonstrate processing of data that is unlawful even where the legitimacy and necessity of processing is justified. Inviolability however often relies on individuals to pursue cases, and workers are often already vulnerable and may have no resources to bring cases to trial, further putting privacy and data protection at risk.

4.2. Inference vs reputation

The right to reasonable inference sits in tension with the range of decision-making capabilities made possible with new technologies of investigation and measure. *Inferred* or *derived* data is data whose exact categories are not explicitly made transparent to the data subject, but where decisions are made or conclusions about reputation are established based on such data. Thus, inferences and decisions can be made about a data subject which are not entirely accurate, nor agreed by a subject and can therefore be classified as being both non-transparent and potentially, highly discriminatory. This can have direct, and unfair, implications for people's reputations. The GDPR gives a data subject the right to query inferences made about them such as reification (Art. 16), erasure (Art. 17), objection to processing (Art. 21) and the right to contest any decision-making and profiling based on automated processes (Art. 22(3)). There remain significant barriers to a data subject's rights with regard to derived and inferred data, nonetheless (Wachter and Mittelstadt 2019: 37).

4.3. Work vs life

Digitalisation has led to mobility of working spaces and a notification-based work culture, where the 'intimacy of work' (Gregg 2011) has led to the uneasy sense of the removal of a separation of life and work for many workers. The private and public sphere are increasingly difficult to separate, and such things as social media usage (see Thompson et al 2019) and wider questions about health are now part of human resource discussions. The rise of the open plan office is one example of the public/private sphere collapse, which paradoxically led to people's increased reliance on e-mails and online collegial socialising rather than the traditional 'water cooler' conversation.

Life and work are increasingly interconnected precisely because of the expansion of digital tools and applications for workers, where the analogue and the digital are not always easy bedfellows. While a worker would not consent to having a line manager continuously stand behind her in an office cubicle, she may be asked to consent to allowing all of her emails to be read; telephone calls recorded; keystrokes quantified; movements around a physical workplace as well as outside the

office and in variable workspaces such as cafes, libraries and even the car watched; and even emotions, sentiment, heartrate, and footsteps tracked and monitored. So much technology and equipment re now supplied by the employer and used by the employee at home that the work/life divide is sometimes difficult to identify (Rosengren and Ottosson 2016), which is exacerbated in the contemporary moment where governments across the world have required non-'key' workers to work at home rather than risk transmitting Covid 19 unknowingly.

The Xora productivity app for example allows companies to collect information on their staff after working hours and wherever they go. It is effectively 'an all-seeing Argos Panoptes, albeit one that seduces us with its novelty and distracts us from its surveillance aspects with a user-friendly interface' (Ajunwa et al. 2017: 142). This kind of tool can lead to algorithmic management and 'digitalised management methods' current author Moore has written about elsewhere. Digital management methods include 'the normalisation of interruptions and expansion of working time in offices' and the ''always on' culture of work and boundary permeability, where workers are expected to be available by phone or email throughout the weekend and evenings, and related practices and expectations' (Moore 2018b: 3; see Moore and Joyce 2020). The blurring of boundaries, however, does not mean management has an automatic right to view that data, or that personal data is generally up for grabs. Truck drivers' GPS software, in many cases, cannot be turned off nor muted, so relevant management teams can constantly identify drivers' whereabouts and contact them even when off-duty, or during sleeping breaks (Levy 2015). Some organisations' IT departments are able to track workers' internet activity while they are staying at a hotel, if they are using a laptop that was provided by the organisation (The Economist 2009). As noted in the Case Study on Nigeria, workers' safety is protected through GPS tracking of delivery trucks, where workers are at risk on highways of robbery. In many cases, of course, the rationale for tracking more than what once understood to be necessary or plausible is not entirely unfounded.

But in 'Worker Privacy in a Digitalized World under European Law', Custers and Ursic (2018) raise important questions about data privacy of workers. Four new practices stand out as being perhaps most invasive around privacy questions, which cloud the separation between what should remain in the private sphere which was once understood as 'life', and work, those being:

1) chip implants

2) social media assessments of prospective employees

3) algorithmic assessments of employee performance, and

4) health assessments via wearables. (Ibid.)

Large data sets gathered from the relevant sources i.e. from social media sites, use of work devices and information gathered from wearable technologies to the extreme cases of chip implants, paired with new data analytics techniques, create significant possibilities for monitoring and tracking workers both inside and outside of the traditionally understood workplace.

Chips sewed under the skin are more common in Sweden than other countries. In the Sweden country Case Study presented in further chapters, people are even using chips to use the national railway system and in one start-up community, to enter co-working spaces. Sweden intends to be a cashless country by 2023 and chips could be part of this drive (Schwartz 2019). Executive director at Harvard's Berkman Klein Center for Internet and Society Professor Urs Gasser, warned that this innovation could encounter more obstacles than enthusiasts in Sweden may be considering. Gasser commented that: 'This experiment has so far happened in a wealthy country, among very digitally savvy people. And while having a chip may play out nicely for well-educated people in Sweden who are part of a digital hub, I question how this will play out for, say, a worker in a warehouse' (Ibid.). Sweden, however, also enjoys the right to co-determination in labour law, therefore it might be more difficult than expected to allow chips to penetrate workspaces and indeed, workers' skin itself.

In 2017, a Wisconsin based vending machine company offered chip implants to workers as part of a marketing technique to draw attention to their vision of cash-free vending machines. Forty-one workers volunteered in the scheme, and the 'chipping party' was reported internationally. Public reactions in the USA were quite strong, however, and even some church groups feared the chip perhaps represented the 'mark of the beast' (Ibid.). Gasser mentioned that the negative public reaction could also be understood as symbolic of the worker/boss power imbalance and a move toward fully dehumanising workers. He stated that: 'Seeing employees get implanted at the workplace made people question what it means to be an employee. Are you a person being paid for your work, or are you the property of the company you work for?' (Ibid.). Dr Ghislaine Boddington ran a session called an Implant Party for Nesta's FutureFest event in London in 2016, where Hannes Sjoblad, a biohacking and human augmentation specialist, sewed chips under the skin of two volunteers' hands which could interact with other digital devices, demonstrating the emerging interest in such activities. The corporeal aspects and the blurring between work and life made possible by digitalisation of work and new tracking methods are dealt with extensively in Moore (2018a), where it seems that soon, employers will be able to track even workers' blood, sweat and tears. Given this level of possible intervention, it is hard to consider how a worker could be seen to meaningfully consent to such activities, if or where they are invited by management to agree to such types of activities.

4.4. Consent in the employment relationship (coercion plus consent)?

Questions about how informed consent can be gained have been consistently part of the debates, as the GDPR is rolled out. As discussed in the GDPR chapter, the concept of consent does not sit easily with the nature of the relationships between workers and management, for quite self-evident reasons. Workers in all kinds of sectors within the capitalist wage labour framework rely on salaries for basic survival, and may feel compelled to consent to things they would not consent to otherwise.

The concept of consent was defined within the 1995 DPD (EU 95/46/EC) as 'any freely given specific and informed indication of his[/her] wishes by which the data subject signifies his agreement to personal data relating to him[/her] being processed' (EU 1995). The GDPR definition goes further, where the way that consent is sought, and given, is now also under scrutiny. The GDPR's Art.4(11) now makes it clear that consent is: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Art. 7 and recitals 32, 33, 42 and 43 of the GDPR provide guidance for the ways the Data Controller (usually the organisation or institution which employs workers and collects data about them) must behave in order to attempt to meet the main elements of the consent option for lawfulness. Recital 32 of the GDPR provides particularly good clarification building on Art. 4 as quoted above:

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Consent to data collection by a consumer, however, is not equivalent to the consent to data collection from a worker. Indeed, 'freely given', can only exist in a situation where a data subject has an authentic say and a real choice. Recognising this, the 2020 update published by the EPDB outlined below indicates, 'if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid'. Furthermore, if it is 'bundled up' and 'non-negotiable' or whereby a subject cannot refuse or withdraw consent without detriment, then consent has not been freely offered (EDPB 2020: 7). The UK ICO's 'Guide to the General Data Protection Regulation' had already warned that 'public authorities and employers will find using consent difficult' and that 'employers and other organizations in a position of power are likely to find it more difficult to get valid consent' (ICO 2019). Worker representatives from unions and works councils have continued to stress, however, that consent is paramount in situations where workers are tracked and monitored (Wild 2017).

In the British Academy/Leverhulme project carried out by the present author in 2015–17, the company which carried out the 'quantified workplace' experiment was queried by a Data Protection Authority. While employees had consented to participation in the project, the Authority asked the company: 'can there ever be a consenting relationship between an employee and employer?'.

The legal basis for the concept of consent does not appear to always be compatible with the basis for 'legitimate interest'. If an employer can infallibly prove a commercial *interest* is salient, the employer can process personal data even when it might be considered an invasion of privacy grounds under normal circumstances (Custers and Ursic 2018: 335). The Art. 29 WP 2/2017 Ch. 6.2 on Data Processing at Work includes this extremely insightful phrase:

> Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances. (Art. 29 WP 2017: 21)

The concept of consent consistently arises in the discussions around data protection and legal collection and processing of people's data. Without explicit tools to ensure that the concept of consent is achieved, the already existing basis for a hierarchy within the employment relationship can continue. There are, therefore, tough issues to consider when thinking about consent and the worker's position in the employment relationship. Among them is the reality of informed consent where there are too many requests for consent, and consent is complex and lengthy, the feeling that there is no real choice – 'consent is often framed as a take-it-or-leave-it offer' (Custers 2016). Further to these problems, consent is rarely renewed, even though user's preferences may change. Nevertheless, a data subject's informed consent is typically the legal basis for processing personal data outside the workspace.

In the context of rapid changes in data capture and analysis, one way to deal with the question of worker consent to data collection and processing is by giving data subjects the right to change their minds. This could help them fully be aware of the consequences of their consent, in a way that the technically existing right to withdraw consent does not. There are significant database management issues that must be resolved. There are a range of complexities surrounding having data deleted; the recurrence of existing problems concerning the number of requests; the length and scope for choice; and the possibility that Data Controllers will not delete the data at all. Custers argues that providing specific expiry dates for consent would reduce the risk of function creep, would raise awareness, and pave the way for a greater range of preferences over data use (2016). Further to this, providing workers with not only the means to withdraw consent, but to also control any surveillance software or hardware tracking their work, and the inviolable right to opt out altogether.

Where data consent is impossible, it is also said that transparency can have justifiable means. No discussion has been held on the question of *how much* knowledge is necessary for transparency to be fully and meaningfully achieved; nor whether there is an inherent virtue nor interminably successful outcome for workers when transparency is attempted. Meaningful dialogue and transparency are certainly important for consent to be achieved, but is it a real substitute for consent?

In a study run by Stanton and Farrell in the 1990s, some workers were given control over the electronic performance monitoring as well as knowledge about how it works. Findings demonstrated that participants who had more knowledge about the monitoring felt they had *less* personal control than those who did not know the specific details about the monitoring (Stanton and Farrell 1996). Nonetheless, 'control' over data collection and processing and their components has become a feature of updated discussions about consent into 2020.

Indeed, on 4th May 2020, the EDPB published an update of the Art. 29 WP guidelines on consent under Regulation 2016/679 (WP259.01) that had been endorsed by the EDPB at its first plenary meeting. The update, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1', emphasises the point that consent is 'one of the six lawful bases to process personal data, as listed in Article 6 of the GDPR' (EDPB 2020: 5). The Guidelines 05/2020 go on to emphasise, however that:

> …requirements for consent under the GDPR are not considered to be an "additional obligation", but rather as preconditions for lawful processing. (EDPB 2020: 6)

The prescient update and the emphasis upon consent as something that should be considered a precondition for lawful processing is encouraging. The Guidelines further place responsibility of the Controller to ensure data collection and processing practices are within these legal parameters and support the protection of personal data and indicates that it must carefully consider what might be the appropriate grounds for processing personal data. Consent can only be considered a lawful basis, this update reads, if the 'data subject is offered control and offered a genuine choice with regard to accepting or declining the terms offered or declining the without detriment' (EDPB 2020: 5). This update grants, of course, that it is difficult to achieve valid consent where there is an inherent power imbalance. On that basis, consent is not always seen as the best choice for managers to ensure the legality of data collection and processing, but the updates within that Guideline are encouraging and provide some grounds for continued discussions. The author of the current report advocates for a continued debate on whether it can be achieved, such as through better collective governance over data processes and reconsidered for any data collection, and usage, in explicit communication with trade union, works councils and other worker representative groups.

The next section looks at a further example of where worker tracking and seeming intentions, in the end, created frictions around what is acceptable for tracking and monitoring of workers, even if what is being tracked is consented to by workers, gamified and part of wellness and wellbeing initiatives.

4.5. Work, agility and the quantified self

The present author Moore's 'Work, Agility and the Quantified Self' was funded by the British Academy and the Leverhulme Trust. Moore's funding allowed her to research a workplace-organised experiential data tracking project which the company itself entitled 'The Quantified Workplace' and ran from 2015-2016. The company which organised the experiment was a small and medium enterprise (SME) of workplace design consultants, which was about to join a much larger multinational corporation. Nearly 50 workers overall joined the project. Workers, who were mostly professional designers and consultants, were provided FitBit Armbands which measured heartrate, sleep and steps taken; were given the app, Rescue Time, on their computers (a software that monitors screentime, composition and other categories within various labels of productivity); and the subjects offered data using a daily lifelong email that asked questions about workers' subjective

stress and perceived productivity on weekdays. All data was viewable to all participants as well as management, located on a shared screen, or 'dashboard', where data from each data silo could be analysed across chapters. So there was a form of transparency embedded, where all workers and managers, who were all participants in the project, shared all data.

The rationale for the project was to enhance workers' health, fitness, and wellbeing. The CEO of the company told Moore that they wanted to make a clear link between health and productivity, and to identify what she called 'billability'. This is akin to the processes of necessity seen in the GDPR. Proportionality between workers' data rights and the importance for the company was not explicitly addressed in communications with workers. All workers technically opted in, simply by volunteering to participate in the project, which was not explicitly required. People who signed up were expected to wear the FitBits at least during the day and many wore them at night. In interviews, workers indicated that they were quite heavy and made sleeping somewhat difficult.

The main findings Moore gathered were that workers were at first, happy to give data to their managers on an individual level and for all the findings to be transparent. By the end of the project, however, participants began enquire whether the data would or might be used for performance management. Workers also became sensitised to their own sense of privacy. One participant stated that: 'It confirmed my thoughts, which I had in the beginning. It is better to change your behaviour based on your feelings rather than a device'. Another participant indicated that: 'after monitoring my workplace behaviour over a couple of months I found out that it didn't change a lot' (Moore 2018a).

4.6. The Live Well, Work Well (L3W) Project

This chapter covers one large project called The Live Well, Work Well (L3W) Project. The Project is called an 'Innovation Activity'.[3] L3W presents an online platform that is intended to stimulate fitness activities for workers to improve their overall health by combining AI, gamification and internet of things (IoT) devices like Fitbit. Researcher Patricia de Paiva Lareiro interviewed the project leader of L3W Luca Foti on 26/11/2019, primarily with the intention of identifying how work and health are linked via technological tracking tools and how workers respond to such projects. During the 16-month project, two pilot studies were conducted with 3 to 4 companies in each study. Doctors monitored the health status and developments of participants. The evaluation of the project had not finished at the time of the interview writing. Mr Foti indicated that some of the questions about workers and companies' responses were not yet known.

The project description indicates that (bold font is for emphasis on areas that link most closely to the themes of the present report):

> The project 'Live Well Work Well' (L3W) results in an online platform whose aim is to promote a better lifestyle among employees, in order to support health prevention, while providing occupational doctors with improved tools to monitor workers' health - and at the same time ensures proper privacy. From a business perspective this is reasonable, as healthier people are more productive at their workplaces. To reach this goal employees are encouraged to do a set of fitness activities every week that are suggested by a recommender engine that was trained by occupational doctors. These also monitor the vital parameters (and improvements) of employees through the platform and are available for direct interactions. To further motivate the execution of these suggested activities a tailored gamification approach selects game elements that should be most effective for the individual employees.

[3] Innovation Activity is supported EIT Digital, a body of the European Union focussing on innovation, entrepreneurial talent and digital technologies.

Researchers on the project first prepared a clinical questionnaire with occupational doctors, asking for personal information regarding the clinical status of the employees. A goal was to automate the profiling of employees' health status with AI. For that, they considered osteoarticular, cardiovascular and metabolic risks, which are categorised into the levels of low, medium or high. Doctors provided the questionnaires and labels. The doctors do not have to see the filled out clinical questionnaire, and the analysis is based on AI, so the employees can use the platform right away.

As a second component, project researchers formulated a recommender system to suggest fitting fitness activities to the users. Foti indicated that: 'When you have done your clinical profile, you have access to some fitness circuits that are good for your profile'. The fitness circuits have been created by occupational doctors. Foti noted that: 'In the first week e.g. you have walking activities, but you can also decide the kind of activities you want to perform. for example, in week 5 you can choose between walking for 20 minutes or having a swim. The doctors provide the information on the equivalents, the choice is based on your taste.'

In the project, the recommender system is trained using AI systems, to analyse users' preferences from past choices, so that the fitness circuit for every week were based on employees' preferences. The clinical profile assigned by the first model can be modified by the doctors at any time, so they can change things based on the results, and also the employees can also edit options any time. By design, every employee can see their own information, but other employees can see only the gamified parts, e.g. how many points someone has collected with their activities.

To use the application, firstly, a user registers and fills out a clinical questionnaire. After submitting this, the AI engine processes the questionnaire and provides users with a clinical profile. Based on this the AI accesses the available fitness circuits and returns the 'most pleasant circuits' to the employees. What the employees see is that they click the button to submit their questionnaire, and then they see the dashboard with a profile and a fitness circuit assigned. Doctors and employees can change the chosen activities. At the end of every 6-month circuit, employees are sent the clinical questionnaire again in order to update their profiles.

At the beginning of the pilot studies, employees were assured that the company would not have access to their personal profiles or their individual activity. There have been no reports on privacy issues from employees who participated in the pilot studies. One project finding shows that workers like the gamification components and reported that it helps them to motivate themselves for the fitness activities. Foti commented that 'They say the gamification component is really a good point to perform fitness activities, earning points, having a leader board, and also there is a Tamagotchi game element (…) We provide a bunch of game elements, and everybody can be interested in one or all. They are interested in such a platform.'

Using the project data, participating companies are provided with a report based on the aggregated data from all their employees. Mr Foti noted that 'We provide them with a report, e.g. this month there has been 300 logins, and there have been 200 completed fitness activities of the 1000 that were prescribed to individual employees'. Companies are not provided with individual information, but they only see aggregated information, like the overall engagement rate, usage rate of the platform within their company and how many fitness circuits have been performed on average. Individual information like weight or cardiovascular risk is only visible for the employees themselves and for doctors. There is no option to see the individual activity or health status of one employee. This also applies to the gamification aspects of the project. Foti commented that 'they don't see user XY played a lot and is on top of the leader board, because we believe this can also be a tool for companies to perform actions to their employees, If they see something, it's only on average and aggregated'.

There are upsides to corporate wellness programs, but there are also significant downsides. Indeed, some say that they 'are creating guilt and anxiety in employees' (Berinato 2015). André Spicer, who wrote *The Wellness Syndrome* with Carl Cederström (Cederström and Spicer 2015), indicated in an interview that:

> …one big wellness program we looked at led previously happy employees in a stable job environment to become anxious about losing their jobs. It seemed to make them think they needed to be more attractive to their employer, and if they did something like smoking a cigarette, they felt it affected their employability. (Berinato 2015)

Wellness initiatives are increasingly involving surveillance measures and this is, not surprisingly, beginning to affect the employment relationship in a number of ways (see Employment Relationships chapter).

The next chapter outlines a series of country specific case studies providing summaries about which technologies are used in respective countries, national law on worker surveillance and data protection, the role of worker representatives, and local examples.

5. Country case studies

For this report, legal and health and safety experts in eight EU states and two non-EU states have contributed to country case studies which report on the legal frameworks in labour and data protection and privacy, and health and safety legislation, within their countries. Given the report asks explicitly what laws are being applied across various EU countries to address worker tracking and monitoring but more explicitly, how they are applied and what the relevance for that area is, the case study approach is considered appropriate.

The necessity to protect business assets from theft, misuse, and exposure to cybersecurity vulnerabilities, and so on, gives some appropriate legitimacy to worker monitoring. While these reasons in themselves are not necessarily inappropriate, they bring about new questions concerning one's right to a private life and communications. These days, the principles within Art. 8 of the ECHR are usually put in combination with principles of good practices in the labour market across Europe. In assessing whether a certain measure is in breach of the principle of good practice, national courts ideally seek to balance the interests of the employer against the integrity and dignity of the worker. Debates oscillate around the ambiguity between a workers' rights to some privacy at work and the employer's right to put boundaries and regulations around the use of work property. This refers to such things as internet communications, social media use, tracking technologies for performance measurement and so on, and whether or not these practices cohere or contradict the right to a private life in general terms.

Similar to the United States, Europe relies on a pragmatic approach to conceptualising employees' and workers' privacy based on identifying the legitimate interests at stake, and practices that interfere with individuals' private lives. The foundations of the European concept have evolved by coupling the protection of privacy with anti-discrimination claims, unlike in the US. This means that the right to privacy is already construed precisely enough to provide concrete privacy rights for individuals in employment. It also strengthens their force in the moral and political discourse. However, the porosity of the European framework stems from an evident lack of clear and contextualised rules governing the scope of protection of privacy rights (Otto 2015). In particular, the legal principles delineating its scope of protection are not sufficiently clear and autochthonous in the context of employment relations to overcome the factual dependence of employees' privacy expectations on the discretion of employers.

This chapter provides a range of insider views from a number of EU and two non-EU countries, which are useful for identifying why companies collect data about workers, what rights workers have, and how case law reflects prescient debates. We outlines a series of country case studies mostly inside the EU, but also in Norway and Nigeria. Legal researchers have provided information that identifies which tracking is common in countries' locations, and for what purposes; which legal and trade union frameworks have been used in these locations; and some accounts of legal cases that have emerged.

5.1. Belgium

Prof. Dr. Frank Hendrickx, who is based at the University of Leuven Institute for Labour Law (KU Leuven Instituut voor Arbeidsrecht), provided the following comments on the Belgian situation. In Belgium, the most common forms of worker monitoring and tracking are cameras/CCTV, mainly for security reasons, but they are also used to monitor work processes. The other common forms of monitoring are badge systems showing attendance and presence at work (as well as in specific rooms and work areas); software monitoring of internet and e-mail; and lastly GPS and location data monitoring seen in the transport and services sector.

The right to privacy is a fundamental right, laid down in Article 22 of the Belgian Constitution. This reads as follows: 'Everyone has the right to respect for his private and family life, except in those cases and under such conditions as indicated by law.' The objective of monitoring is, in principle, to keep the proper functioning of the company or workplace intact. This is usually included in the codes of practice that companies have drawn up on the subject of data use and monitoring. The Belgian National Collective Agreement no. 81 supports this and states that monitoring is permitted for the purposes of keeping a check on 'faithful observance of the policy and rules in force within the company on the use of online technologies' (Art. 5, §1(4)). Monitoring of electronic online communications data is permitted only in so far as it fulfils the principles of legitimate purpose and proportionality and also maintains the principle of transparency, as ensured by the procedural conditions (Art. 4).

Apart from this, the Agreement also permits monitoring for one or more of the following objectives:

- the prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity;

- protection of such of the company's economic, commercial and financial interests that are confidential, and also the discouragement of practices that conflict with them;

- the security and/or efficient technical operation of the company's IT network systems, including associated cost control and also physical protection of the company's equipment (Art. 5, §1(1–3)).

In addition, the commentary accompanying the aforementioned Agreement states that the possibility of monitoring communications data for training purposes remains unaffected, since it does not constitute surveillance. In other words, this Article does not give a restrictive list of objectives but a very broad use of wording that permits the company to carry out monitoring. Art. 5, §2 states that the employer must define the objective(s) of monitoring clearly and explicitly. In other words, the objectives must be clearly and explicitly included in the company code of practice.

5.1.1. National Collective Agreement No. 81

In Belgium, the National Collective Agreement No. 81 of 26 April 2002 (on the protection of employees' personal privacy with respect to the monitoring of electronic online communications data, concluded within the National Labour Council and extended by Royal Decree of 12 June 2002), is the only instrument which deals specifically with access to and use of online communications facilities at work and the monitoring of such use.

The National Collective Agreement No. 81 specifically only applies to the private sector, and hence not to the public sector. This clearly leaves a huge vacuum for the public service. However, criminal provisions of the Criminal code (Article 314bis) and the Belgian Act on Electronic Communications of 13 June 2005 additionally protect confidential communications. Exceptions can be made to monitor communications between third parties only on the basis of consent, or a legal provision. Whether an employer is a third party, or whether employees can/need to give their explicit consent, is subject to discussion.

It is sometimes assumed that the principles laid down in Articles 16, 17 and 18 of the Contracts of Employment Act of 3 July 1978 apply as the pre-eminent expression of employer and employee obligations in the context of the employment relationship. This Act can be seen as a legal basis for employers to monitor, including telecommunications. As an agreement that has been decreed to be generally applicable, the National Collective Agreement no. 81 is legally enforceable.

5.1.2. Scope

The objective of National Collective Agreement no. 81 is to safeguard the fundamental right of employees to have their personal privacy respected in the employment context by specifying, while at the same time taking account of, what is required for the company's efficient operation, the purposes for which a system for monitoring communications data may be installed, the conditions of proportionality and transparency with which it must comply and the rules governing the permissibility of individualizing such data. The Agreement is without prejudice to more favourable provisions at sectoral joint committee or company level (Article 1, §1). The Agreement also does not relate to rules on access to and/or use of a company's electronic online communications facilities, which are the prerogative of the employer. It therefore leaves intact any applicable company rules and practices on information and even consultation in this field. It is also without prejudice to existing company rules and practices regarding trade union activities (Article 1, §2).

5.1.3. Definition

For the purposes of applying the aforementioned Agreement, 'electronic online communications data' means electronic online communications data sine loco, irrespective of the carrier medium via which something is transmitted or received by an employee in the context of employment (Article 2).

5.1.4. Commitments Undertaken

The signatories to the Agreement, i.e. the recognised social partners, affirmed the following principles:

> - the employee side acknowledges the principle whereby the employer has the right to exercise control over tools and equipment and their use by employees in the context of the performance of their contractual obligations including, subject to the rules on applicability laid down in this agreement, circumstances where such use falls within the sphere of the employee's private life;
>
> - the employer side respects the right of employees to the protection of their personal privacy in the employment context and the rights and obligations that result therefrom for each party (Art. 3).

5.1.5. Proportionality

National Collective Agreement no. 81 states that the monitoring of electronic online communications data may not, as a general principle, entail any intrusion on the employee's personal privacy. Where monitoring nonetheless entails an intrusion on the employee's personal privacy, this intrusion must be kept to a minimum.

Informing employees to achieve transparency should ideally be ensured by involving a works council or a trade union. An employer intending to install a system for monitoring electronic online communications and other types of personal data collection must inform the works council of all aspects of that monitoring (Art. 7, §1), and more particularly:

- the policy on monitoring and prerogatives of the employer and the supervisory staff;
- the objective(s) pursued;
- whether or not personal data are stored, and where and for how long they are stored;
- whether or not monitoring is to be permanent. (Art. 9, §1)

Where there is no works council this information must be given to the committee for prevention and protection at work or, in the absence of such a committee, to the trade union committee or, if no such committee exists, to the employees and workers concerned (Art. 9, §2).

5.1.6. Individualisation of online communications data

The National Collective Agreement no. 81 lays down rules on the individualisation of communications data. Firstly, the Definition 383 indicates that for the purposes of the agreement, the 'individualisation' of electronic online communications data means an action whose purpose is to process data of this kind collected during monitoring installed by the employer so as to make it possible to attribute such data to an identified or identifiable person (Art. 12, §1). Depending on the objective of the monitoring system installed by the employer, the individualisation of data takes place either as a direct procedure, in accordance with Art. 15; or as an indirect procedure, in accordance with Art. 16 and Art. 17. An indirect procedure is one that is combined with a prior notification phase (Art. 12, §2).

Secondly, with regards to procedural conditions, the direct individualisation of electronic communications data is permitted in all cases where monitoring is aimed at one or more of the broad objectives specified in Art.5, §1 (purposes 1 to 3) (Art. 15). The purpose of Art. 5 is to offer an employer who in pursuing the objectives, detects an irregularity the opportunity of proceeding directly, in light of the general data available to him, to the individualisation of electronic communications data, in order to be able to trace the identity of the person or persons responsible. Individualisation can only take place indirectly when the monitoring is relating to the observance of company policies with regard to the use of the internet or e-mail.

Art.5, §1 (purpose 4) also indicates that individualisation of electronic communications data is sometimes permissible, but only if a prior notification phase is fulfilled (Art.16, §1). The purpose of prior notification is to inform the employee(s) clearly and comprehensibly that an irregularity exists, and that electronic communications data will be individualised if any new recurrence of a similar irregularity is detected. So, only in case of a second violation of the company rules, individuals can be detected, and consequently measures can be undertaken against them.

On 16 June 1998, the National Labour Council concluded Agreement no. 68 on the protection of private workers' lives as regards video surveillance at work. While taking into account the International Labour Organization's Code of Practice on workers' privacy and Belgian legislation, the social partners wanted to define the specific safeguards with respect to surveillance. They agreed to introduce mandatory consultation and information disclosure on video surveillance in firms.

The Agreement covers all video surveillance systems, whether or not the pictures are kept, and specifies four authorized purposes for which they may be used:

- health and safety;
- protection of the firm's property;
- monitoring the impact of machinery or workers on the production process; and
- monitoring workers' output.

In relation to the first three purposes, video surveillance can be permanent, although if the monitoring of the production process is carried out on workers, (for instance to improve the organization of work), surveillance should only be temporary. The Agreement specifies that surveillance should be appropriate, relevant and not excessive with respect to the objective, and that it should not intrude into private life.

In fact, Agreement no. 68 imposes an obligation to inform the works councils or the trade union committee on the introduction of the surveillance, stating the following:

> …the purpose of the surveillance;
>
> whether or not pictures are kept;
>
> the number of cameras and where they are placed; and
>
> the operating periods.

Second, it imposes an obligation to consult the same bodies if it appears that video surveillance might have an impact on the worker's private life. In that event employers are required to reduce intrusion to a minimum.

As outlined, Belgium is quite advanced in data protection law and therefore will not need to make many changes to accommodate GDPR regulation requirements.

5.2. France

When it comes to worker surveillance in France, new technologies are contributing to an evolutionary leap from a direct control by management to a multifarious system based on various data collected through remote and digital scrutiny. Asst. Prof Antonio Aloisi, who is based at IE Law School, IE University, Madrid, prepared this brief on the French case. Dr Aloisi indicated that according to Fresh scholar Francis Kessler, '[t]he development of information and communication technologies, if badly managed or regulated, can have an impact on the health of workers'. The French Labor Code, the Law 'Technologies and Freedoms,' the case law and the GDPR define a framework for conditions and restrictions on the use of technologies at the workplace.[4]

Employers are responsible for compliance with health and safety measures, and liable for any tort committed at work by any employee under their direction. The employer can control employees in order to assess their skills and competences in case of possible recruitment. Art. L. 1121-1 of the French Labor Code states that 'no one shall limit the rights of the individual, or individual or collective freedoms, unless the limitations are justified by the task to be performed and are in proportion to the goal towards which they are aimed.' The protection of the employee's personal life represents a limit to managerial prerogative: controls must be done without jeopardising the employees' human dignity. Workers have a fundamental right to private life. The Court of Cassation stated that that 'the employee has the right, even at the time and place of work, to respect for her privacy, which implies in particular the confidentiality of communication (Court de Cassation, Chambre Sociale [Labor Division of the supreme court] October 2, 2001, No. 99-42.942 (Fr.). If the employer fails to comply, not only can she not use the evidence gathered, she may also face criminal conviction or administrative sanctions.

Three principles govern computer surveillance and collection of data on employees in the French Civil Code: the principles of transparency or loyalty; proportionality; and relevance. This means that the workforce must be informed about surveillance devices before introducing it. Any restrictions placed upon employees must be justified, proportionate to the aim pursued and relevant. Case law has developed a jurisprudential limit to the power of surveillance. First and foremost, one of the restrictions resides in the principle of loyalty towards the workforce in the implementation of the system controlling their activity.

There are two main methods of monitoring the employee. A 'direct' control of action that is visible to the eye of management is legitimate (Soc. 26 April 2006, J.C.P. S. 2006. 1444, note Corrigna-Carsin.

[4] This paragraph draws from Aloisi and Gramano (2019).

Soc. 26 Nov. 2002, Dr. soc. 2003.225, note Savatier). However, if the employer wishes to install a specific surveillance device, a mandatory conciliation procedure laid down in Art. L. 1121-1 must be followed based on information, delivered to both the individual (Code du travail [C. Trav.], art. L. 1222-4) and the workforce as a collective unit. A number of formalities must be complied with prior to implementing any monitoring of employee emails. Amongst other things, the employee representatives from works councils and health and safety committees, must be consulted before implementing any system which is capable of monitoring employees' activities, and employees must be informed thereof.

In particular, no system of surveillance or data collection may be installed without prior notice to employees and their representatives (Code du travail [C. Trav.], art. L. 1222-4 (Fr.). *See* Vigneau 2002). The employer has to consult the works council over any introduction of new technology within the company if this might affect employees' working conditions, employment, pay, training, and qualifications (Code du travail [C. Trav.], art. L. 2321-38. Art. L. 2312-38 LC, Art. L. 2328-1 LC). The *Comité social et économique* has to be informed about new techniques or automated systems of personnel management allowing for the surveillance of employees' activities before their implementation, as well as their modification, on penalty of inadmissibility of the collected evidence. In addition, employees must be informed personally.

According to Art. L. 1224-4 LC, no information concerning an employee personally can be collected by a device that has not been previously disclosed to her. As a consequence, by interpreting Art. 9 of the Code of civil procedure in conjunction with Art. 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms and the principle of loyalty, evidence obtained without the information or consent of those involved is illicit. Tools performing or allowing personal data processing are no longer to be 'declared' to the *Commission Nationale Informatiques et Libertés* (France's National Commission on Computing and Liberties, CNIL). Before 2018, a simplified or normal declaration, or even a prior authorization scheme had to be carried out. In case of failure to comply with these provisions regulating surveillance, the employee could refuse to be monitored by devices. Today, instead, a compliance and self-control system apply. The CNIL operates a compliance control *a posteriori*.

On a positive note, after a pioneering discussion among scholars, the 'right to disconnect' was made law in 2016 (Article L.2242-17 of the Labour Code). At the company level, the right to switch off has to be recognised. Additionally, firms must design procedures to implement this provision aimed at ensuring the respect of rest periods and enabling a protected work-life balance. Further to this, in 2019 the Commission Nationale Informatiques et Libertés (France's National Commission on Computing and Liberties, CNIL) published new guidance on the appropriate use of biometric facial recognition to comply with the French privacy and human rights protections. The CNIL clarified that consent, control of data by data subjects, transparency, the right to withdraw from the service, access to and the security of biometric data are requirements to be met.

5.3. Germany

Daniel Weidmann is a Berlin based lawyer specialising in collective labour law with *dka Rechtsanwälte Fachanwälte*. Weidmann aided in the preparation of the German case here, indicating, first of all, that Germany is partaking in globalised free markets. Therefore the procedures and devices employed to monitor worker performance and behaviour should be similar to workplaces in other industrialised democracies. Generally speaking, video cameras; silent monitoring or key word spotting; and mediate/indirect monitoring procedures and devices are all used in Germany. The latter refers to monitoring as a by product of procedures that are not directly aimed at monitoring but nevertheless allow for the comprehensive processing of performance and behaviour related worker data. Examples would be e.g. any computer software that collects individual data or a GPS system in a company car.

5.3.1. Highest rates of worker monitoring in Germany

The highest rates of worker monitoring in Germany is predominantly within call centres, but the banking sector, logistics/delivery and other branches are monitoring workers heavily too. With digitalisation becoming more and more important, immediate as well as indirect monitoring routines have become commonplace, even in workplaces which formerly were disinclined to use such practices two decades ago – think small mechanical workshops or care homes for the elderly. From Weidmann's experience, in areas without co-determination, misconduct is widespread.

5.3.2. Legal restrictions for monitoring workers

While the GDPR and its German counterpart (BDSG) are meant to protect employees on an individual labour law level, these regulations have proven less than fully effective so far. As Art. 6 par. 1 b) GDPR allows the processing of worker data if the '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', many day to day data processing activities in an employment must be considered legal under the GDPR. Other regulations such as the ban on profiling measures in Art. 22 GDPR or the right to revoke ones consent according to Art. 7 par. 3 GDPR are very helpful in theory, but require courageous individuals to push these rights through in front of a labour court.

5.3.3. Collective Labor Law

Collective Labour rights should work very well in Germany, because Works Councils elected by all staff members are granted strong legal co-determination rights. According to sec. 87 par. 1 no. 6 of the German Works Constitution Act (WCA), 'the introduction and use of technical devices designed to monitor the behavior or performance of employees' requires prior consent between works council and employer. This has proven to be an effective way to abolish the most abusive practices of worker monitoring and to limit the negative effects of procedures and devices.

Any device that allows for the processing of individual behavior- or performance-related employee data is considered an 'electronic device' In terms of sec. 87 par. 1 no. 6 WCA. Monitoring workers must not be its primary function. So any operating system on a personal computer, a GPS system, a transponder access key system or an ERP system (such as SAP), can qualify as 'electronic device' and be subject to co-determination, as long as it processes data of identified or identifiable individual employees or a small working group of employees.

5.3.4. Co-determination in day to day industrial relations

As works councils are well aware of these rights and labour courts do not hesitate to issue cease and desist orders to employers who fail to observe these regulations, co-determination of electronic device use is commonplace at least in bigger organizations.

Ideally the use of these co-determination rights leads to agreements on the usage of specific devices that specify the regulations of data processing, e.g. what data is processed; to what end is it gathered; what are worker protection rights in case of abuse; agreement on timelines for data storage and erasure; authorisation concepts, and much more.

5.3.5. Case Law

As the German legal system heavily relies on codified law, case law has not got a similar significance as e.g. in Anglo-Saxon legal traditions. The rulings of the different German high courts are nevertheless very important for the exegesis of all existing regulations. Their case law helps with the interpretation of abstract codes of law. Also, even in Germany some aspects of life remain unregulated. Here the high courts' decisions help filling gaps the legislators left.

1983 Census Ruling of the Federal Constitutional Court

In its late 1983 census ruling, the German Federal Constitutional Court acknowledged a new 'unwritten' fundamental human right to informational self-determination on the grounds that the democratic principles of society are endangered if a person concerned by modern data processing has no say in such processing. According to the Federal Constitutional court, a person who does not know about the data processing or cannot influence what information concerning his behavior is being processed and stored will be adapting his behaviour out of caution ('panoptism'). This does not only affect individual freedom of action, but also the common welfare, since a free democratic society requires a self-determined participation of all its citizens. (BVerfG v. 15.12.1983 - 1 BvR 209/83 u. a.). As a consequence, no data processing is considered to be irrelevant. Any such processing requires a justification and a legal basis.

The Federal Labour Court's fundamental decision on monitoring devices

In late 1983, the Federal Labour Court ruled that, despite the rather clear wording of sec. 87 par. 1 no. 6, WCA which indicate that it is not only technologies that are 'designed' to monitor the behaviour or performance of the employees which are subject to co-determination. According to this and all subsequent court decisions, a technical device is already relevant for co-determination if it allows for such monitoring, even if this is just a side effect of the device and not its principal purpose (BAG v. 6.12.1983 - 1 ABR 43/81). This court decision has defined modern data protection co-determination and led to countless lawsuits and collective labour law agreements on the use of specific electronic devices.

5.3.6. Examples of misconduct

German employers are, daily, severely breaching Data Protection Regulations, so it is very hard to pick a single example. Under the GDPR and the new German Federal Data Protection Act (BDSG) even a google research of a candidate for a vacant position can be considered illegal at it cannot be considered 'necessary for hiring decisions' according to sec. 26 par. 1 BDSG. Concerning collective labour law, any introduction and use of technical devices without prior agreement with the works council must be considered a misconduct, if the devices allow for monitoring the behaviour or performance of the employees.

5.3.7. The role of workers' representatives

As outlined above, German works councils have the task to monitor whether the employer observes all legal regulations according to sec. 80 par. 1 no. 1 WCA. This obviously also includes the employer's compliance with data protection law. Workers can insist on the observation of their co-determination rights according to sec. 87 par. 1 no. 6 WCA. Whenever the employer fails to find an agreement with the works council prior to any introduction and use of technical devices allowing for monitoring the behavior or performance of the employees, the works council may immediately seek an interim injunction in front of a German labour court. Many works councils use this option in order to delay the introduction of technology that they consider harmful for staff. The mid- to long-term goal of most works council activities in the field of data protection is the creation of works agreements that forbid the most harsh (ab)use of monitoring options modern technology grants at the work place and set very clear and specific rules for any legal use of the devices in question.

5.3.8. Germany's Response to the GDPR

Germany has reacted to the GDPR by passing a new Federal Data Protection Act that specifies some abstract clauses of the GDPR and makes use of some gaps deliberately left open by the European Regulation. One example for the latter would be the criminal provisions of sec. 42 BDSG. Since the legal system of the European Union does not allow for criminal provisions on the European level, these had to be included in a national regulation. One example for the former would be the German

regulations on the Data Protection Officer (DPO) in sec. 38 BDSG that make use of Art. 37 par. 4 GDPR that allow individual member states to specify additional facts that require employers to designate DPOs.

5.4. Netherlands

Legal Expert Dr Beryl ter Haar of Leiden University provided guidance for the Netherlands country Case Study here. She indicated that there seems to be a rising trend in performance management in the Netherlands. This is especially the case in information and communication technologies where there is a shortage of workers. Instead of having yearly or twice yearly performance evaluations, they are taking place on a much more frequent basis, sometimes every two weeks. Although presented as rather informal, this practice also involves the registration of information about the workers at a more intensified level.

Dr ter Haar quoted the Authority on Personal Data Protection website which indicates that the following forms of worker surveillance are operational in the Netherlands:

- Covert cameras;
- Telephone centres;
- GPS-systems;
- Software to prevent RSI;
- Filter software to control the use of e-mail and internet;
- Systems registering presence, working time and access;
- Badges or chipcards designed to follow access, presence, movements and/or payments.

Dr ter Haar researches the construction and agricultural sectors, where drones can be used as surveillance devices. Drones can gather information to protect materials, monitor and protect wildlife, e.g. protecting nests of ground breeding birds, young deer from big machines used to work the land, and for advanced precision fertilization of the soil. With regards to robotization and real time production monitoring, in the agricultural sector robots are used for harvesting, particularly in green houses. Workers working side by side with robots experience real time monitoring.

The main legislative rules about monitoring derive from the GDPR, but the Netherlands has not adopted further rules for the employment situation as allowed for by Art. 88 of the GDPR. In addition, Art. 8 of the ECHR applies. However, in its rulings on the right to privacy and employee monitoring, the European Court of Human Rights has shown itself sensitive for the regulations by the EU. Since there is no specific regulation based on Art. 88 of the GRDP, there is no formal role for workers' representatives other than case law confirming that the conditions for consent (Art. 7 GDPR) are better, or at least more seriously, ensured when the works council has also consented to the monitoring. Of course, this would be limited to general monitoring, but not in a very specific, individual case in which the employer has e.g. a strong suspicion of misconduct, which can be best proved by monitoring data.

One regularly returning issue in the Netherlands is whether the employer had properly informed his employees that he would monitor, how he would monitor and did he get their consent to monitor? Being in a subordination relationship per definition it is considered that the employee cannot ever really freely give his consent for monitoring activities. In jurisprudence from the lower courts especially, it is regularly considered that when the works council has given its consent, and the employee has also consented, the employer is now more transparent, and has taken the conditions for consent more seriously into account.

5.5. Nigeria

Ehi Iden is the Chief Executive Officer for Occupational Health and Safety Managers in Lagos, Nigeria.[5] Mr Iden expressed the safety and security benefits of worker tracking in various industries. The first concern for managers in Nigeria is *whether people come to work, when and where* people are working, and ultimately, *how* they are working. Various types of software can identify these things, and often sit in the background of work devices, whether laptops, smartphones or in trucks, cars and motorbikes.

Another very important concern for managers and OSH officers is the security of workers in Nigeria who are working in high risk areas. From 2008 – 2016, there was a great deal high level of kidnapping of workers in Nigeria. Thus, tracking workers thus had added safety benefits. Security of drivers as well as passengers is protected in platform applications such as those used in Bolt, Uber, O-Ride and Gokada. A few stories about taxi driver incidents against passengers raised awareness of these issues and the security features extend beyond workers in these cases. Another security risk is hijacking of petroleum transport trucks with products and diversion of such trucks by the driver. Trucks are often diverted and looted by drivers. Mr Iden indicated that the government should be taking a much more active and conscientious role to deal with the emerging security risks in all these cases, and work to regulate these.

A very common tracking activity involves keeping an eye on the speed of drivers and motorcycle riders. For example, Mr Iden while working on an Industrial Hygiene project for a client in Southern Nigeria, he noticed that one large company uses speed 'guns' to monitor the speed of trucks and other official vehicles used by employees on a route from the town to the cement factory along a road lined with settlements, where children often played.

How do you balance profit with safety? Mr Iden asked, and then commented that if you put profit before safety and you have litigations to deal with as a result of accidents, you may be instantly blocked from your very market due to losses and reputational damage. So, safety should be the primary incentive for tracking workers at all points. Data protection law is not strong in Nigeria and nor are unions. However, workers are usually trained well and understand why tracking is implemented. In that light, Iden stressed, the benefits of monitoring should work for all.

5.6. Norway

Case study a) **Norway and Natural Environment Workplaces**

Tone Lyse is the Occupational Health and Safety manager for the Norwegian Environment Agency. Ms Lyse provided information for this Case Study with the focus on The Environmental Agency in Norway, which has about 100 rangers whose primary task it is to patrol and protect nature and wildlife. Snowmobiles are used for patrolling and Norwegian law permits tracking the locations of cadavers, but not GPS tracking of workers' routes, unless safety and health reasons are strong enough to justify the tracking of humans. However, wildlife-spotting cameras are installed to record and monitor the activity of predators, e.g. wolverines in the vicinity of den entrances. Recorded material which is irrelevant according to the purpose of the installation is destroyed afterwards, thus not accidentally recording any humans who may be out in the wilderness.

Another aspect of a ranger's job is to track e.g. wolverines to locate the dens and sometimes eliminate mothers and their offspring to keep the population down to a determined threshold. Animal culling is controversial and den locations need to be kept protected. Another issue faced is the security vulnerabilities that large collections of data always introduce with for example, a

[5] Interview carried out with Ehi Iden by Moore, 18/10/19.

database designed to store and standardize observations of wildlife under the threat of extinction. If a regular citizen observes e.g. an owl, one can enter information about spottings into an app and record the animal's exact location, sex, activity etc. But these birds and their nests are also very popular among criminals, who want to carry out taxidermy on rare animals for the black market. It is important to keep this data from the public for the most part, because of the risk of theft. This is done by lowering the degree of location specificity, and by delaying publication to the public interface concerning locations.

Case study b) **Norway and Wider Industry Workplaces**

Another industry where tracking and monitoring are carried out in Norway is in waste collection. Tone Lyse mentioned a court case about worker tracking in Norway in 2012 involving a waste collector. The company Retura Sør-Trøndelag used a GPS tracker on the company's garbage truck to see where/when garbage is emptied. However, the company used the data to analyse the overtime claims and the worker was fired for apparently falsifying overtime. The labour union took the case to the Norwegian Data Inspectorate who ruled that the company was allowed to use the GPS overall, however, the company had not told workers that it may be used to check working time, and the action was deemed illegal, - the company was fined an infringement fee of NOK 100,000.

Dr Gunn Robstad Andersen is a Senior Adviser for the Arbeidstilsynet (Labour Inspectorate) in Norway and provided further information about the case. He indicated that GPS tracking devices are used on ambulances to identify location. Other tracking tools are used to measure response time to assignments and time spent on call-outs as well as static time. In home care, personal digital assistants are required to register time that care workers spend at a patient's house, amount of time travelling and when they leave. Cleaner monitoring is done in a similar way. In retail, surveillance is carried out in a number of ways including for example a 'secret customer' practice, whereby someone will leave the correct amount of cash on a counter and walk away before it is entered into the cash register. A camera will film the worker to see whether they register the purchase correctly, or not. In carpentry, plumbing and electrician work, digital platforms monitor performance, which is then made available for clients. In call centers and service personnel work, calls are recorded and often, customer feedback is sought for the service provided.

There is an increase in technological equipment available in Norway which enables employers to monitor and track employee behaviour and performance. The media presents stories concerning both tracking and performance monitoring from time to time; employees feeling controlled and monitored, describing how this is perceived to be stressful and illegal; employers' registration of the time employees spend on the toilet; cameras, earplugs and walkie talkies used as instruments for the employers to instruct employees in a sort of remote control way in what to say and how to behave towards customers; apps enabling customers to evaluate haircuts, and service, but which can be misused by customers for sexual harassment, to name a few. Advertising commercials use the results of performance monitoring of the work done by carpenters, or plumbers etc., and make these results visible for clients who can then 'pick the carpenter who has received good evaluations – a 6 star-worker'.

National Norwegian law about worker tracking includes the Working Environment Act where Chapter 9 gives employers the opportunity to implement control measures at work, with the proviso that there must be a factual reason for them. In order to, for example, set up a camera, there has to be a stated purpose. The law sets requirements for discussion, information and evaluation of the control measures. The employer also has an obligation to discuss the need for, design and implementation of, such measures with the worker representatives. Indeed, workers should know the purpose of the measure, its consequences and its estimated duration. Workers have the right to know that they are being monitored and why they are being monitored.

The Norwegian Working Environment Act, Chapter 9-2 lists requirements for consultations, information and evaluation of control measures as follows:

1. The employer is obliged as early as possible to discuss needs, design, implementation and major changes to control measures in the undertaking with the employees' elected representatives.
2. Before implementing such measures, the employer shall provide the affected employees with information concerning:
    a. the purpose of the control measures,
    b. practical consequences of the control measures, including how the control measures will be implemented,
    c. the assumed duration of the control measures.
3. The emp loyer shall, in cooperation with the employees' elected representatives, regularly evaluate the need for those control measures that are implemented.

The GDPR now requires employers to communicate with workers what data is being collected about them and why as well, and Norway has taken the introduction of the GDPR very seriously, because it is subject to these regulations even as an Associated country rather than an EU member (as are all other countries who intend to work with EU countries). Tone Lyse, who was the Privacy Officer at the time that the GDPR was rolled out from May 2018, noted in our discussion that Norwegian legislation was already very worker focussed. Key principles of the GDPR already existed in its legal frameworks. Nevertheless, a lot of attention is being paid to the GDPR anyway, to ensure compliance, and to make any related changes.

5.7. Slovenia

Mojca Prelesnik is the Information Commissioner for Slovenia. The Information Commissioner is responsible for the supervision of personal data, and the courts decide on broader aspects of the protection of the rights of the workers to the protection of privacy and to the privacy of correspondence. Ms Prelesnik provided information about her country's situation regarding worker surveillance for the current report. Firstly, Ms Prelesnik indicated that the highest rates of worker monitoring in Slovenia are present in the private sector, such as in banks and insurance companies and are much less prevalent in the public sector.

In Slovenia, based on the information office's inspection practices, the following worker monitoring practices prevail:

- video surveillance
- monitoring of location/movement within office spaces
-tracking of worker's arrivals/departures (via record cards, biometrics)
- monitoring of phone calls
- audio monitoring (e.g. recording meetings)
- monitoring of email usage, also after termination of employment
- monitoring of internet usage to depict cyberslacking
- monitoring of printer usage
- motion control when using corporate vehicles (GPS)

In Slovenia's national legal system, there are not many very specific legal restrictions about monitoring workers. However, the Employment Relationships Act provides general provisions on which personal data the employer is allowed to request from the worker; provision on the existence of workers' privacy; provision on protection of personal data, and the like. In one legal case (n. Pdp

49/2011), the Court decided that the protection of privacy of correspondence also covers the emails and files saved on the hard disk of workers' computers.

Ms. Prelesnik has in numerous cases found illegal implementation of video surveillance and illegal processing of traffic data. Based on the proposed provisions of the new national Personal Data Protection Act (ZVOP-2) that has not yet been adopted, workers' representatives must be consulted before introducing video surveillance. Art. 111 (on video surveillance inside workspaces), Para 5 of ZVOP-2 states that:

Before introducing video surveillance in a public or private sector entity, the employer must consult with all social partners, including worker representative trade unions and works councils. The consultation shall take place within 30 days or within another longer period specified by the employer. Upon receipt of the opinion, the employer shall decide on the introduction or non-introduction of video surveillance. These provisions are similar to the Personal Data Protection Act as adopted in 2004, and later amended in 2005 and in 2007 (specifically Art. 77 para. 5).

5.8. Spain

Francisco José Trillo Párraga, Prof Dr. of Labour Law and Social Security at Castilla-La Mancha University, provided the information for this Spanish country Case Study. In recent times, the use of video surveillance at work has prevailed as an instrument for monitoring labour compliance in Spain. Other forms of electronic control of workers have included the uses of e-mail control, remote tracking techniques by GPS, social nets tracking, computer registration, phone call tapping, tracking of internet usage and customer satisfaction assessments. The Spanish experience shows a great variety of industries that resort to electronic controls and video surveillance systems, but it is in the textile and food and small and medium trade businesses where a more frequent use of these systems is found.

In terms of national law, the Spanish legal system has a number of regulations to restrict worker surveillance. Some amendments have recently been made which influence the rights of workers in relation with monitoring systems which were secured by the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. This has to do with the protection of natural persons with regard to the processing of personal data and on the free movement of such data that repealing Directive 95/46/EC. Art. 88 of the GDPR indicates that States shall ensure the protection of the rights and freedoms in relation to the processing of personal data of workers in the field of employment. In particular:

> These rules shall include appropriate and specific measures to preserve the human dignity of data subjects, as well as their legitimate interests and fundamental rights, paying particular attention to the transparency of processing, the transfer of personal data within a business group or a union of undertakings engaged in joint economic activity and workplace supervision systems.

In the same way, Art. 22.5 of Spain's Organic Data Protection Law states that:

> Employers may process data obtained through camera or camcorder systems for the exercise of the supervisory functions of workers provided for in article 20.3 of the Workers' Statute, provided that these functions are exercised within their legal framework and with the limits inherent therein. Employers will have to inform workers about this measure. In the event that the images have been captured by the flagrant commission of a criminal act, the absence of the information referred to in the preceding paragraph shall not deprive the images of probative value, without prejudice to the responsibilities that may arise from such absence.

However, this text has been modified by LO 3/2018 parliamentary amendment presented by the Parliament Confederal Group Podemos-En Comú Podem-En Marea, proposing far more stringent controls, including these restrictions:

> The installation of video surveillance cameras or any device that allows the capture of images of workers will always require, without exception, that the employer informs in advance in an express, precise, clear and unequivocal way to the interested parties and their representatives about the existence, location and particular characteristics of such systems. Under no circumstances shall the capture of images be allowed for direct or indiscriminate control of workers. The consent given by the workers or their representatives shall not be sufficient in any case to alter the provisions of this paragraph.

In the absence of specific legislation regulating the use of technological and digital means in the field of work and due to the limited provisions contained in collective agreements, case law has itself progressively set guidelines. Both the Spanish Constitutional Court (TC) and the Spanish Supreme Court (TS) are influenced by the ECHR. Nevertheless, case law has developed with many changes and controversies. Initially, the lower courts recognised without restriction the surveillance and control measures in the company on the basis of the argument of the 'public dimension' of work arenas. However, from 2000 onwards, the Constitutional Court (STC 186/2000) initiated a doctrine based on the need to use the triple judgment of: necessity, suitability, and proportionality, in cases where fundamental workers' rights could be affected by control measures used by employers.

STC 241/2012, influenced by the judgment of the ECHR Copland vs. UK and Halford vs. UK cases, and the doctrine of the Spanish Supreme Court (STS 26th September 2007) adopted the criterion of reasonable expectation of confidentiality (*expectativa razonable de confidencialidad*). This criterion means that if an employers' activities do not meet basic objectives of information transparency, then 'reasonable expectation' might be violated. In its STC 29/2013 ruling, the Constitutional Court began to divide up the effect on the right to privacy on the one hand, and the violation of the right to the protection of personal data on the other. After this judicial pronouncement, it was interpreted as mandatory for the employer to inform the worker in advance of a surveillance measure, where:

> Previous and express, precise, clear and unequivocal to the workers of the purpose of controlling the work activity to which that recording could be directed. Information that had to specify the characteristics and scope of the data processing to be carried out, the recording time and the purposes. (Tribunal Constitucional de España 2013)

For a brief period, the *reasonable expectation of confidentiality* was connected to the right of workers to receive this kind of information, in all cases where in addition to the worker's privacy right also personal data protection could be affected. However, in its rulings SSTC 170/2013 and 39/2016, the Constitutional Court changed its own doctrine, in light of the first ECHR judgment in Bărbulescu I. Spain's Courts sought to strengthen the employer´s right to media ownership, exempting the employer from its obligation to inform the workers, in the terms quoted above, considering 'sufficient' to be symbolised by a sticker of label warning of the situation of video-surveillance zone.

Thus, the TC understood that industrial relations were an exception to the employer's duty of information and the right of workers to consent in situations where they were subjected to video surveillance controls, as long as the purpose is not different from that of monitoring the performance of the employment contract.

The *final* ECHR Judgment on September 5th 2017, also called Bărbulescu II, established better precedents for reasonable expectation of confidentiality, however. The High Court of Justice of Castilla León (TSJ Castilla León) echoed this final judgement on 11/04/18 and clarified that:

> The doctrine of the Constitutional Court and the jurisprudence of the Supreme Court on the prior knowledge by workers of the installation of surveillance cameras have been affected, in the Opinion of the Chamber, by the judgment of the European Court of Human Rights of 9 January 2018. (ECHR Judgment in López Ribalda and Others vs Spain, 1874/13 and 8567/13)

The right to freedom of enterprise, recognized in article 38 of the Spanish Constitution, subsumes or integrates the right to private property (Art. 33 Spanish Constitution). The freedom of enterprise includes, in turn, the faculties of management, organization and control of labour activities that take place in the production process. So, ultimately, it is this right that legally legitimizes the employer's power to control and monitor labour activity. Much of the TS jurisprudence, as well as the most recent TC, strengthens the right to private ownership of the means of production, putting the security of the means of production before the fundamental right of workers to privacy.

Broadly speaking, the regulation provided for in LO 3/2018 provides for legislation that places in a subsidiary place the collective supervision of workers' representatives, highlighting the individual aspect of the worker's privacy. However, there are many doubts about the role of trade unions and workers' representatives. Above all, collective bargaining is the great absentee in the puzzle of workers' digital rights. That is why the bill adds a final article (art. 91) which, under the heading of 'digital rights in collective bargaining', generally prescribes that 'collective agreements may provide additional guarantees of rights and freedoms related to the processing of workers' personal data and the safeguarding of digital rights in the workplace', a legislative mandate that seeks to save the reproach against a rule that makes the effectiveness of the right to privacy pivot, private life and protection of the images and sounds of workers, about the design that the entrepreneur makes about the direction and control of any business activity.

5.9. Sweden

Asst. Prof. Dr Caroline Johansson of Uppsala University and Assoc. Prof. Dr Vincenzo Pietrogiovanni of Lund and Aarhus Universities are labour law experts. These two scholars provided information for the current report about the Swedish situation regarding monitoring and tracking workers.

In Sweden, the tools for monitoring and tracking involve the following devices. Badges for accessing offices or other places and spaces of work are used to track working time of employees as well as their movements throughout. Software tools are installed in employees' electronic devices, including laptops, smartphones and GPS devices. GPS monitoring is common in transport, carpenters/electricians and painters' jobs in Sweden. Video worker surveillance is common in banks, stores, buses, and trains. Electronic systems are set up to enter and exit, or logins on computers are very common in many other sectors. Further to this, drug and alcohol tests are administered in transportation and energy industries.

It is also worth mentioning microchip implants which have gained the attention of the international media. In Sweden, implanted chips can work as swipe cards, to open doors, operate printers, or buy food and beverages at the company café (The Washington Post 2017). A Swedish start-up hub offered to implant its own workers and other start-up members with microchips in 2017, which was popularised in the tech sector quite quickly. Since then, many people in Sweden have started to implant themselves with microchips, for instance, to pay for public transportation (Savage 2018; Schwartz 2019). So far, microchip insertions are entirely voluntary and not as widespread as other monitoring measures at work, but the practice has sparked significant international interest.

The purpose of monitoring and tracking workers in Sweden matters to legislation and case law, where the purpose of monitoring should be connected to the safety of a peculiar business such as, for instance, a nuclear plant; it matters in the health and safety of employees and/or customers, for example calculating working time or discourage crimes against banks or stores; it matters as well in

the rehabilitation of sick employees. Swedish case law around privacy and invasive tracking practices reveals two sets of interests for judgements: 1) focus on the workplace, which requires an overcoming of the integrity of employees for reasons of safety, and 2) the protection of a company's property rights. Of course, tracking and monitoring devices can be used for other purposes. This is where Swedish legislation and the trade unions are of most importance.

5.9.1. Legislation on worker surveillance

In Sweden, there is no single comprehensive piece of legislation concerning the monitoring of workers. Though there have been several public inquiries (SOU 2002:18, SOU 2009:44, SOU 2016:41, SOU 2017:52) in which the need for regulation has been pointed out, but the Swedish legislator has not yet adopted any special act on the matter. The large case law on such matters in Sweden mainly concerns the possibility of employers to undertake drug and alcohol tests on their employees. Apart from drug and alcohol tests, there are cases regarding inspections of employees' bags, and body searches when leaving work. All these cases have led to fervent debates amongst Swedish scholars and has instigated a general public debate. Indeed, in a proposal for a trade union strategy for surveillance at the work place, Landsorganisationen (which is the confederation of blue-collar workers commonly called 'LO'), proposed that trade unions should ensure that collective agreements on drug and alcohol tests should limit the measures the employer is allowed to use, and that rehabilitation should be given to workers who do test positive for drugs or alcohol. In fact, one drug testing case was taken before the ECtHR in 2004, in a case brought by a Swedish cleaner employed at a nuclear power plant who claimed she should not have to be drug tested at work. The ECtHR ruled the applicant's case to be inadmissible, thus upholding the rulings Swedish Labour Court had done earlier in the domestic case, in which the employer's right to conduct drug tests was found justified by the special nature of the workplace.

The right of employers to monitor their workers can be derived from the employment contract, or from collective agreements. If the issue of worker tracking has not been regulated by any of those sources, such a right is usually considered as based on the principle according to which any employer has the right to take managerial decisions and, therefore, the employer can lead, control and eventually sanction their employees. These are generally referred to as employers' managerial prerogatives. The employers' prerogative has a strong position in the Swedish legal system, and it could be argued that the underpinning principles behind them are connected to the right to property and the right to conduct business.

However, sources can be restricted by statutory law (through imperative rules connected to the protection of a general interest) and by the so-called 'principle of good practice on the labour market' (in Swedish: *god sed på arbetsmarknaden*). The relevant legal framework on surveillance and worker monitoring in Sweden is made of different statutory sources. Firstly, the EU's GDPR is relevant for storing and organising data, so if the employer has, for example, used cameras in a lawful way to monitor the business in question, the GDPR poses restrictions on how the data from the cameras can be used, stored and what information should be given to the employees. Secondly, a particular relevance in Swedish legislation is played by Art. 8 and, namely, the line of case law regarding worker privacy, which fixes limits to the employers' possibility to monitor their employees' e-mail correspondence. Thirdly, the Swedish Criminal Code provides, in its Fourth Chapter, rules on crimes against a person's freedom and peace. In particular, it establishes prohibitions against abusive filming and photographing (Chapter 4, § 6a).

In order for a measure to qualify as abusive filming or photographing, such filming must be unlawful, made in secrecy, and/or made in a private area such as a changing room. Hence, if cameras are visible, and there is clear and evident information regarding the surveillance, or if there is an agreement on camera surveillance, it was not perceived to be abusive according to the Criminal Code. Nonetheless, this does not necessarily prevent a possible breach of Art. 8 of the ECHR. There are also other, more detailed rules regulating camera surveillance in the so-called Camera

Surveillance Act, which applies to surveillance of areas that the public has access to, such as stores, banks and public transportation.

In Chapter 4, Section 6c of the Swedish Criminal Code, there is a prohibition against integrity intrusions that focus on spreading photos or information that are sensitive. Chapter 4, Section 8, moreover, continues with a prohibition against unlawful access to mail correspondence. Finally, in Chapter 4, Section 9a, there is a prohibition against monitoring conversations with the help of technical equipment such as, for example, tapping phones. The regulation presupposes that this is done in secrecy similar to the abusive filming mentioned above. It should be noted, however, that the Criminal Code is a general piece of legislation, and none of the above-mentioned provisions, address employers specifically. Therefore, the Criminal Code does not create any obligations for employers that do not always apply also to the generality of individuals in Sweden. Since the employer has a larger possibility to monitor computer traffic, phones etc., this puts them in a situation of being more likely to be exposed to handling sensitive data connected to the privacy, liberty and dignity of employees. This is the reason why in Sweden, both the GDPR and ECHR Art. 8 are used as legal limitations on what employers can do.

5.9.2. Collective Agreements

In Sweden there is no Labour Inspection institution nor authority. For health and safety matters for example, the Swedish Work Environment Authority (Arbetsmiljöverket) carries out inspections in order to enforce domestic legislation on safety at work. In negotiations for new collective agreements in 2016 in Sweden, trade unions sought to include both clarifications about when electronic control measures could be used, and about mandatory consultation when any technology for control mechanisms is introduced, with a health and safety lens. The demand came from 6F, a collaboration between the trade unions for construction workers, electricians, painters, real estate workers, cleaners, and janitors; together with SEKO membered by several professions such as transport, mail delivery and the like.

Where the employer is bound by a collective agreement, a trade union party has the right to negotiate. It also has the right to receive current information. Swedish law enables trade union officials to perform trade union duties on working time, both regarding labour law and health and safety. Hence, trade unions do, in practice, have a role to play in whether the employer follows the above mentioned laws and the collective agreement. An important measure is to ensure that workers' interests have been taken into account when assessing whether surveillance measures are necessary or not. This indicates that even if it can be argued that there is a need for legislation regarding workers' integrity, the enforcement of existing rules and the prevention of arbitrary use of information about workers is already possible through the trade unions.

If the employer is bound by a collective agreement, trade unions have the right to negotiate when the employer decides to introduce or apply different surveillance measures. Such monitoring measures are usually considered 'an important change' according to Section 11 in the Co-determination Act, which obliges the employer to initiate negotiations. Matters that are not considered an 'important change', or if the trade union is not bound by collective agreement to the employer but has members, it can still be subject for negotiation if the trade unions consider the issue important and call for it. The negotiation process makes it possible for the trade union to scrutinize if the employer has taken the workers' integrity into account and that the measures taken are in line with the laws mentioned.

A trade union may, of course, also try to persuade the employer not to use a surveillance measure even if it would be in line with the law. However, if the trade union and the employer do not agree, the decision is left to the employer in accordance with the employer's prerogatives. There is also the possibility to regulate integrity issues in collective agreements in order to limit or clarify when the employer may take surveillance measurements (compare this with the answer to question 2). It is

also important to note that the above-mentioned laws are not semi-optional as many Swedish labour laws are. Hence, it is not possible to derogate from, for example, the Camera Surveillance Act.

Collective agreements can be concluded on central or on a local level, if they are allowed according to the central agreement. If it is regulated in collective agreement, a trade union can, in the case of a conflict with the employer, invoke the right to interpret the collective agreement until the Labour Court has made its final decision (Section 33 of the Co-determination Act). This can be of use if the employer plans to use surveillance measures in a situation where it is not clear if it is in line with the collective agreement or not.

5.10. United Kingdom

Dr Eliza Watt, Lecturer in Law at Middlesex University, provided the case study for the United Kingdom concerning monitoring and tracking at work. Dr Watt indicated that worker monitoring plays a part in the employment relationship in the United Kingdom for a number of reasons, such as to make some checks on the quality of work produced by the employers' staff; to safeguard workers from unsafe working practices; to satisfy a legal or regulatory requirement to carry out some monitoring; to protect their own interests (including from theft) and those of their customers, and to address bullying and harassment concerns.

According to the 2018 report of the Trades Union Congress (TUC 2018) in the UK, 56 per cent of the surveyed workers thought it likely that they are already being monitored at work. 72 per cent of workers surveyed believe that it is fairly likely that at least one form of worker monitoring is occurring. Workplace monitoring was recorded as being more prevalent in relation to young workers (age between 21 and 35), and employees in large companies. 66 per cent of workers are concerned that surveillance could be used in a discriminatory way if left unregulated. 70 per cent thought that surveillance is likely to become more common in the future. The report stresses that trade unions should have a legal right to be consulted on, and agree in advance to the use of electronic monitoring and surveillance at work, and finally, the government should ensure employers can only monitor their staff for legitimate reasons that protects interests of the workers (TUC 2018).

Workplace surveillance is any form of employee monitoring by an employer. It has occurred in various forms in the past, including bag checks, signing of timesheets and keeping a close eye on the employees. However, with the advances in technology it has become more complex and pervasive, comprising mainly the tracking of employees' computer/ telephone use and their movements. The most common types of the former surveillance methods include 'monitoring employees' emails from their work account and browser history/or files saved on work computers, browser histories on personal devices that are connected to the employer's Wi-Fi network, using webcams on work computers, use of social media outside of working hours (such as monitoring the posts on an employee's personal Facebook or Twitter account)' (TUC 2018: 4). In addition, 'employers also use keystroke-logging software to monitor when and how much an employee is typing and keep records of employee telephone logs and calls, together with recording their calls' (TUC 2018: 4).

The latter, tracking employees' movements, involves, *inter alia*:

- the use of CCTV,
- tracking the location of company assets, e.g. by use of location trackers on company vehicles, computers or phones,
- using facial recognition software to monitor the expression and mood of staff while working,

- security and bag checks when entering and leaving the workplace,
- using access cards to monitor and record the location of employees in a building and how long they spend there and
- using handheld or wearable devices to monitor and record the exact location and movement of employees within the workplace. (TUC 2018: 4-5)

The changing nature of surveillance has been noted in the energy sector, where the TUC observed an increasing trend towards excessive surveillance through the use of vehicle monitoring technology and dash cameras, together with real-time streaming video surveillance in some vehicles. A number of companies have begun to demand that body cameras be worn and web-based apps used to control particularly those workers fitting smart meters (TUC 2018: 6).

5.10.1. Worker Surveillance Legislation

Workplace monitoring is widespread and likely to increase. Although employers may and do

conduct worker surveillance, these practices are subject to legal restrictions applicable to

CCTV monitoring, monitoring of IT systems and electronic communications (such as employee mails), searches and drug testing. To that end, three often overlapping legal regimes can be distinguished aimed at protecting workers from excessive and intrusive monitoring which apply to the UK case, some of which are already covered in the current report. These are the Human Rights Act 1998 (HRA 1998) and the European Convention on Human Rights 1950 (ECHR 1950); the Investigatory Powers Act 2016 (IPA 2016) together with the Investigatory Powers (Interception by Businesses etc for Monitoring and Record Keeping Purposes) Regulations 2018 (Regulations 2018); and the Data Protection Act 2018 (DPA 2018), alongside the current GDPR.

The Human Rights Act 1998, which came in to force in 2000, sets out the fundamental rights and freedoms applicable to everyone in the United Kingdom. It incorporates the rights enshrined in the European Convention on Human Rights into domestic law, which means that:

> if an individual's rights have been breached, he/she can bring the case directly in the British court rather than in the European Court of Human Rights (ECtHR)
>
> all public bodies must respect and protect human rights
>
> all new laws must be compatible with the Convention rights and
>
> courts, as far as possible, must interpret laws in a way that is compatible with the ECHR rights.

Art. 8 of the European Convention on Human Rights indicates that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others. (Note 6: Art 8)

Lawful interception of communications in the UK is governed by the Interception Powers Act 2016 (IPA 2016), which seeks to provide the legal basis for undertaking surveillance by public bodies as required by Art 8 ECHR. Section 3(1) of the IPA 2016 makes it a criminal offence for a person to intentionally and without lawful authority intercept in the UK any communication in the course of its transmission if that communication is sent via a public or private telecommunication system or a public postal service. Section 6 sets out what constitutes 'lawful authority', providing, *inter alia*, that interception must be authorised pursuant to a warrant (IPA 2016: s6), which may relate to (a) bulk powers to intercept (IPA 2016: Ch1 of Part 6); (b) the obtaining of bulk personal datasets (IPA 2016: Part 7); (c) equipment interference (IPA 2016: Ch3) and (d) communication data acquisition and retention (IPA 2016: Ch2).

One circumstance, whereby interception is lawfully authorised under the Act is provided for in s46, which allows it where it is undertaken by business and other bodies for the purposes of monitoring and record keeping (IPA 2016: s46). Section 46(2) states that such interception is lawful only when authorised by regulations made by the Secretary of State. Pursuant to this provision the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations has been issued in 2018. The Regulations provide the legal bases pursuant to which a body, such as a company or public authority, may intercept communications for monitoring, or record keeping purposes that are transmitted by a telecommunications system they control (Regulations 2018: s3). The Regulations' Explanatory Memorandum (Explanatory Memorandum 2018) sets out a number of justifications in relation to the need for such interception based on legitimate business activities, including:

> …establishing whether individuals, such as company staff, who are using the relevant telecommunications systems are achieving the standards required by their company in the course of their duties, to detect the unauthorized use of the relevant system,
>
> to ensure the system is working effectively, to monitor communications made to confidential counselling services, which are free and which permit users to remain anonymous if they so choose (Explanatory Memorandum 2018: 7.4)… where certain public authorities are authorized to undertake warranted interception under the IPA 2016 (Explanatory Memorandum: 7.4) [and] in the interests of national security in order to, for example, test and assure the security of their own systems for cyber-attack. (Home Office UK 2018)

Thus, pursuant to the 2018 Regulations, employers are able to intercept communications made through their internet servers, landlines, voicemail and other private telecommunications systems. However, in accordance with section 4 of the Regulations, 'Restrictions on the Lawful Interception of Communications', the interception will only be lawful if:

- it is solely for the purpose of either monitoring or keeping a record (or both) of communications relevant to the carrying on the employer's business activities- s. 4(1)(a)
- the telecommunication system is provided for use wholly or partly in connection with these business activities-s.4(1)(b)
- the employer has made all reasonable efforts to inform every person who may use the telecommunication system that their communications may be intercepted-s. 4(1)(c) and
- in the event that any interception is made to protect national security, it must be made on behalf of a person who is authorised to apply for issue of a warrant in those circumstances-s.4(1)(d).

5.10.2. Data Protection Law and ICO Guidance

Since the introduction of the Data Protection Act in 1998, the UK has had data protection rules that set out strict principles on how personal data can be used by organizations, including employers. As a general principle, personal data must be processed in a fair and lawful way and includes data gathered through worker surveillance such as a person's image on a CCTV recording or information about a person's use of a computer, emails or the internet at work (Note 1: 14). Due to the recent legislative changes, the law regulating when and how employers can carry out monitoring is now set out in Regulation (EU) 2016/679 (the GDPR) (Note 10) and the Data Protection Act 2018 (DPA 2018). The former repealed Directive 95/46/EC and the latter the Data Protection Act 1998 from 25 May 2018 (already covered in the current report).

Together, the GDPR and the DPA form the main legal framework in relation to data processing in the United Kingdom, but they do not prevent employers from monitoring workers. Indeed, they set out legitimate reasons why employers may wish to monitor their workforce and provide that where monitoring and surveillance involves collecting, storing or using personal data, this needs to be done in a way that complies with data protection principles and is fair to workers.

Prior to the introduction of the GDPR and DPA 2018, the UK ICO issued 'Data Protection. The Employment Practices Code' (ICO 2013a) and 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information' (ICO 2013b). These Codes deal with the impact of data protection laws on the employment relationship and aid employers' compliance with, and the interpretation of, the statutory framework contained previously. They also aim to encourage them to adopt good practice. However, at the time of writing in 2020, neither document was updated to reflect the changes introduced by the GDPR and the DPA 2018. Consequently, the 'Employment Practice Data Protection Code, Part 3: Monitoring at Work' should still be considered as good practice in the context of worker monitoring in the meantime.

5.10.3. Some Cases from United Kingdom Courts

In addition to the extensive legal framework regulating worker monitoring and surveillance, there is also an implied obligation of trust and confidence between employer and employee, breach of which may amount to a fundamental breach of the employment contact giving the employee the right to resign and claim constructive dismissal (United Bank Ltd vs Akhtar [1989] IRLR 507). UK courts have interpreted the right to privacy and data protection rather restrictively finding that ecovert surveillance of an employee's home who was suspected of dishonest time records was not disproportionate (McGowan vs Scottish Water [225] IRLR 1670); filming of an employee in public did not breach his right to private life (City and County of Swansea vs Gayle UKEAT/0501/12); and that it was fair for an employer to dismiss an employee based on derogatory comments made about the employer on social media, even though the comments were posted two years prior to the dismissal taking place (BWB vs Smith UKEAT/0004/15).

It remains to be seen how the UK will deal with its imminent departure from the European Union. While it has made great strides in data protection and workers' rights in these areas, it is not yet clear what will occur as this country exits the region.

6. Worker cameos

A series of in-depth semi-structured interviews with workers was carried out specifically for the present report, to identify what is happening inside workplaces and spaces. While the sample size is moderate, the experiences of workers outlined here can be seen as representative of the types of industries within which they work and workers' experiences within them. Most are working in multinational companies and all are based in EU countries. One interviewee is a full-time consultant for an international organization. One works for a travel agent as a customer service representative. One is a dentist. Another worker is a creative director at an advertising agency. One works as a financial analyst for a bank. Two are based in call centers, where one is a customer service manager and one is involved in sales of telephone rates. Another works in the online marketing industry. Two cameos are of content moderators for the largest social networking platform. Three interviewees gave interviews about previous jobs, two of which pre-date the GDPR. Of interest is that many of the workers spoken to have not had the conversations required by the GDPR where transparent communication about the data that is collected about them, and the reasons for its collection are explained, a point which is made very clear in Art. 14 (see GPDR chapter).

This chapter provides cameo descriptions of each interviewee's experiences of being monitored and tracked at work. The questionnaire is included as Appendix I.

6.1. Content moderator

This chapter begins with the cameos of two content moderators who worked for the largest social networking platform in 2015 (pseudonyms Christian and Hannah), in a contact centre in a European country. Both had worked there for two years at this job. These workers' jobs were to view videos, messages and photos before they are posted on the networking platform, to identify whether or not they violated the company's policies. Approximately every week, workers went to training sessions where they learned what was considered acceptable for posting and what was not. It was often quite difficult to mentally retain the policy changes, but workers' accuracy was tracked, and job retention was contingent on a quite high level of accuracy as well as taking enough 'tickets' per day. The number of tickets required was 4,000 a day. These workers used the words 'modern slave', 'prisoner', and 'robot' to describe how they felt. It reminded the present author of the film *A Clockwork Orange*, where the protagonist's eyes are taped open as he is forced to watch violent films. The prisoner dimension was further made aesthetic when tape was placed over the windows so passers-by could not see inside.

Workers were required to create a special profile within the social network databases, which they were required to log in and out of. Indeed, workers had to log out of the system in a particular chapter of the profile in order to go to the toilet, take short breaks, training sessions or going for cigarettes. Targets and accuracy rates were set, and data observed regularly. Indeed, workers were made aware from their first day that they were being tracked and team leaders were constantly present to check progress. Neither worker was asked to give consent for data to be collected about them, but they were told what would happen with the data, i.e. that they would be held accountable and could be fired if their accuracy and speed fell behind quotas too frequently. The accuracy and speed requirements created a lot of stress. Hannah indicated that this was highly demotivating and was one of the reasons she left the job.

Content moderation work is psychologically extremely difficult. Christian indicated that he 'was always stressed and under pressure… we were checking violent content, child sex abuse, self-harming images' and the like. At some point, when cycling home from work, Christian stated, he had a kind of hallucination of a car crash and could actually picture what would happen to the bodies of pedestrians as well as his own body. Due to watching so much pedophilic imagery, the worker

indicated that he started to lose perspective of reality and found himself even starting to change his ways of behaving towards his friends' children, for fear of doing something that might seem even slightly abusive. Violent content images would haunt his dreams. Hannah stated that 'it started as something quite harmless, but it turns out to be harmful work for my mental health' because of the nature of the images and content she was required to look at.

This kind of psychosocial paranoia was exacerbated by the very intensive surveillance monitoring. Hannah and Christian both knew that their work was being closely monitored from day one. Christian indicated that he was constantly aware of being tracked, and stated that surveillance seemed to intensify over the course of the time he worked there. Hannah never felt comfortable at work, she indicated. The combination of the psychologically difficult work and the intensive monitoring and tracking of it, made her feel 'suffocated'. Close monitoring did not help her to work more effectively, but simply gave her 'stress'. She felt that the job made her feel 'more impatient, [have] more anxiety' and eventually, it 'killed [her] motivation to work' and in particular, to work for a big company, she indicated.

People were constantly afraid of being fired and were pressured to work weekends. Indeed, despite only agreeing to work one weekend a month when starting the job, Christian found himself instead working three weekends a month. There was no discussion of worker representation, and only at one point was a union representative made known to workers. Workers were skeptical about the individual and thought s/he was more of a company representative.

6.2. Financial analyst

Christina has worked for one bank in an EU country for around three years. Her working conditions are quite good, with a good work/life balance, and she does not feel she is excessively tracked. She is required to use a personal ID card to come into the building where she works. She has a personal ID to log in to her terminal and a system whereby she has to indicate her arrival and departure times, as well as log out during lunch. Christina is not aware of any other tracking or monitoring techniques of her work, and certainly has not been provided any information about data that is collected, in that light. This bank employee mentioned that she had probably consented at some point to having data collected about her, but that she did not remember.

6.3. Travel agency customer service

James has worked as a customer service representative for a travel company since January 2016. James reported that he experienced good working conditions and a good atmosphere at first, but when a new system was introduced to begin to track his and colleagues' work via such software packages as Atoss and DTM to control working time and identify revenue brought in by each employee, he noticed. James was asked to consent to allowing the data to be gathered, but he was not told why it was being collected. After that, James began to feel less comfortable, feeling that he was being evaluated constantly. He indicated that felt he was being asked now to work for a set of quotas and to make money for the company rather than simply to enjoy his job, which he previously did, when he started this job. He does not know about a union that he could join. His motivation has lowered, he explained, and he just does not feel as happy working at this travel agency as he once did. Data collected about him is now even being used in appraisals.

6.4. Creative director

Candace was the creative director for an advertising agency for 12 years, where she is monitored by a number of apps which are used in order to track workers in this agency. There is also a front desk manager who checks workers' times of arrival and departure. Computer activity is tracked and

Candance indeed, noticed she is being tracked almost all of the time. While she was told data was being collected, she was not told what kind of data, nor was she asked for her consent. However, just knowing that data was being collected created a negative atmosphere at work and tension arose between colleagues so that she felt she could not trust anyone. Over time, Candace realised that the quality of her work was not as important to management as how fast she worked. Indeed, she stated, she had had many horrible bosses over time, and it did not seem to be getting better. One positive end to the gathering of data is that, in appraisal situations, she could prove her working time based on data. In the end, however, Candace indicated that she had a breakdown and finally left that job.

6.5. International organisation consultant

Peter is a full-time consultant for an international organisation, and has been doing this work for around three years. His experience is similar to that of Christina's, where there is no evidence of extensive monitoring or tracking. Indeed, in this international company, consent is only sought from workers when photographs are taken of employees for company publicity or for stories which are going to be published in the media about specific people. Christina, who also works for a bank, and Peter, appear to have the most autonomy of any interviewee.

The manner by which management can know if one is working is through the log-in system with company-owned computers, and there is a trust-based system where workers are required to keep personally derived logs of hours worked. The only times that Peter has realised the organisation knows where and when he is working, at least when he is working in the organisation's building, is when IT services contacts him with enquiries about repairs or updates of the computer he is working on. During the interview for the current report, Peter says he now plans to make an enquiry about what kind of data if any, is being gathered about him, besides his hours, in the absence of discussions on this topic with management.

6.6. Call centre customer service lead

Cassandra is a team leader in customer service for a call centre and has worked for the company since December 2018. Her performance has been tracked since her first day, where Sales Force records work time and productivity. The software Reaper tracks breaks and accuracy. There are also two colleagues whose roles are to check technical skills while working, and to monitor the performance of teams and the team leader's work likewise. Both roles were established to check workers' standards of performance and productivity and were introduced after she started working at the company, in early 2019.

Monitoring and tracking occur constantly in Cassandra's workplace, from the moment she arrives at work, to the moment she leaves. She is, technically, 'asked' to consent to data being gathered about her, she indicated, because she must click on consent notices each time she logs into the relevant software to carry out work. While Cassandra has access to the data being gathered, she has not been told exactly why the data is being gathered or what it is used for. Regardless, data is used in appraisals to point out this worker's weaknesses in performance. Even with all of the software that is available to her, this interviewee indicated that it has been increasingly difficult to organise her working time because of constantly changing work procedures and tracking requirements that align with those. She is not aware of any union or worker organisation she could join. She feels that she has been pressured to work faster. On the other hand, she feels that she can work more efficiently and has found that tracking and monitoring has given her increased motivation to deliver a better service and to demonstrate her skills.

6.7. Call centre front line

John worked as a call centre front line salesperson 2015 – 2016. John was very clear that *all* activity in the call centre was recorded and tracked. From the moment he arrived until the moment he left, John's movements and actions were tracked and monitored. The company also knew how long calls lasted, how long and when breaks were taken, how long workers spend in the toilet. Workers knew this, but were usually surprised how much data was produced about them in aggregate form which was shown during team meetings to indicate sales, performance and productivity scores. Individuals' sales and performance data was always shown on the walls around, so all workers could see each other's information. Indeed, sales calls were not only machine recorded, managers also actively listened in, without first telling workers.

Beyond this, managers also listened to workers when they were not on calls, when people would normally chat about general things like their social lives, while waiting for calls to go through. John indicated that he felt this was an invasion of privacy. Indeed, he and colleagues were chastised for having personal discussions at all, and it became clear that all communication outside of calls, was discouraged. The constant tracking and mistrust from management, John indicated, demotivated him, and made him work more tactically and in a more cynical way rather than encouraging him to do the job better. Indeed, John was so unhappy, he felt compelled to reduce sales in order to be put on probation and maybe even be fired, which meant he was also given a separate room, the upside of which was that the room was much quieter than in the main hall. John indicated that while he was on probation, he was not allowed to take breaks at the same time as the other workers. He was not aware of any union group and stated that he thinks if one had been organised, it would be immediately shut down by a quite heavy-handed management. There are some similarities between John and Christian, who worked as a content moderator, where the stress spilled out into after-work hours and he found he was in a very bad mood and was not able to relax or enjoy life. John was very relieved to leave this job at the end of his contract.

6.8. Industrial designer for an online marketing company

Jean works for an online marketing industry as an industrial designer and has done so since 2012. From the first day, her work was tracked, via a product management tool which tracked how many 'to dos' are done per day, a ticket system, and a time tracking system via fingerprint data. Like most of the others described in the worker cameos, consent is provided technically, i.e. when workers log in to the systems they use to work. In the first instance, however, Jean 'consented' when she signed her contract and there was no choice but to consent, in order to take the job. Over time, the working conditions changed, particularly when a new manager was hired who was more interested in monitoring all projects than previous management. This has created stress and Jean expressed her concern about the key performance indicators that have been introduced. She is also not aware of any union she could join, but a silver lining Jean expressed is that precise work time tracking means she can prove when she has worked overtime.

6.9. Dentist

Tom is a dentist and has been working at a new practice since September 2019. Tom was surprised to find the extent of working time tracking at the new office. There are CCTV cameras and login requirements at seemingly every turn. He has to record hours of arrival and departure, and time taken for breaks. Indeed, Tom's boss even telephones the desk 'spontaneously' (daily), at the time the office should close, to ensure they have not closed early.

Tom was not made aware of what data would be collected about him at work, nor was he asked for his consent. He was not told why the data was being collected, although he can deduce that time tracking is carried out in order to adjust his pay accordingly. Management also listens to conversations and views workers' social media profiles. These practices, Tom stated, cause constant stress, tension and pressure. Indeed, there is a very high rate of staff turnover, and although he has only worked there for a handful of months, he cannot figure out who is new, who is not, who has left, who is a new starter, and so on, meaning there is no teamwork nor chance to establish relationships. There has been no discussion of a union nor worker representation of any kind. Tom feels very demotivated and constantly stressed and continues to work there only for the money. However, he is already starting to question his future in the profession, in part because of the high levels of worker tracking, which he was not expecting in a professional job.

6.10. Discussion

There are some commonalities and patterns across these Worker Cameos that portray increasingly normalised working conditions and employment relationships. But perhaps just as striking, are the contrasts to workers' expressed experiences of monitoring and tracking across industries and professions. One thing that stood out is that workers in contact and call centres are most conscious of being surveilled, and therefore feel the most uncomfortable. However, there are other contexts where monitoring and tracking were more surprising, such as the case of the dentist, industrial designer, and creative director. Nonetheless, all industries seem to be pursuing some kind of tracking and monitoring of workers.

No worker felt that they had been meaningfully consulted about data collection/processing/storage. In all industries in that light there seems to be very little consultation surrounding gaining consent for data tracking, and based on the interviews outlined above, there has probably been no meaningful consent for it. As discussed elsewhere in this report, it is problematic to discuss the concept of consent any time a work and employment relationship is depicted, due to its inherently unequal and imbalanced nature, and in most cases, Workers who 'consented' to data collection only did so by way of logging in to systems within which they worked.

Further to this, no worker interviewed knew of a union nor worker representative organisation that she or he could join. Indeed, the trade union Prospect carried out a survey with 7,500 workers and released the data in early 2020. Results showed that nearly half of these workers are not aware of employers collect about them (48 per cent). 34 per cent are not confident that their data would be used appropriately (Prospect 2020a).

This representative set of interviews demonstrates that worker monitoring and tracking occurs in many kinds of workplaces, not only the stereotypically seen call centers and warehouses. Many workers are aware that they are being tracked all day long, every day. Some methods of tracking are purely embedded in software and others, like the case of the dentist, are mixed methods, as the manager who phones every day at the precise time the office should be closing. The first-person insider view of tracking and monitoring in a variety of professions demonstrates the tentacles of tracking and monitoring as they become increasingly widespread.

7. First principles and policy options

As it has been demonstrated, tracking and monitoring of workers is in no way waning today. On the contrary, there is a significant uptake of technologised practices in new surveillance workspaces. Workers are expected to self-track and to also consent to having extensive data to be gathered about themselves. Indeed, this is set to increase, as home working is likely to become increasingly prevalent after Covid-19 is impacting many industries, where workers' activities and measures of productivity will be further monitored digitally (see Felstead et al. 2002a, Felstead et al. 2002b for earlier research on home working). The research and findings outlined in this report identify where this is happening; how it is happening; the multilevel legal and institutional frameworks both nationally and regionally around the emerging practices as well as workers' direct experiences of surveillance at work. Now, we provide explicit next steps in discussions around policy and practice in worker data collection and its governance, where worker representative groups are front and centre.

This chapter identifies a series of first principles for data protection and privacy at work and then proposes a clear list of policy options which EU member states and international bodies who want to process data in partnership with companies and organisations within member states, should take into account (see Table 1). Overall, companies and local government policy must prioritise interests of workers in a wider remit i.e. the impact that workplace and workspace surveillance has on worker techno-stress and the psychosocial hazards created by data collection and tracking. While the GDPR provides a historically groundbreaking move in the right direction in privacy and data protection for workers, there is of course, far more that needs to happen. This concluding chapter provides an outline looking at a handful of institutional responses within the rapidly changing labour market, where digitalisation practices allow, and are even expected to, monitor and surveil work.

Table 1. First principles and policy options

First principles	Data protection and first principles protections by design and default
	Proportionality, necessity, transparency
	Co-determination
	Prevention over detection
	Collective data governance
Policy options	Require union/worker involvement at all stages
	Introduce and enforce co-determination into labour law in all EU member states
	Businesses to compile certification and codes of conduct
	Prioritise collective governance

7.1. First principles

The Data Protection Working Party Opinion 2/2017 3.2.2 refers to Art. 88 of the GDPR, which states that Member States may, 'by law or *collective agreements* [italics added by present author], provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context' (9). The specific rules, as suggested within the Opinion text, may be decided by collective agreement with unions, and this is strongly recommended by the present author. Data protection rules may be provided for the purposes of:

- recruitment;
- performance of the employment contract (including discharge of obligations laid down by law or collective agreements);
- management, planning and organisation of work;
- equality and diversity in the workplace;
- health and safety at work;
- protection of an employer's or customer's property;
- exercise and enjoyment (on an individual basis) of rights and benefits related to employment; and
- termination of the employment relationship. (Art. 29 WP 2017: 9)

To ensure these rules meet first principles, it is imperative that these rules are intentionally discussed with worker representatives in the form of unions and works councils in all cases. Worker representatives must be present on governing boards in all countries. Worker representatives should be treated as full social partners and contribute to all discussions and decision-making and be given full leeway to ensure these rules are followed. In particular, Opinion 2/2017 states that rules should be designed and provide measures that can safeguard data subjects' 'dignity, legitimate interests and employees' fundamental rights'.

The following first principles have been selected as guidance for European Union states' policymaking to ensure recognition and protection of workers' personal data rights.

7.1.1. Data protection and first principles protections by design and default

Art. 25 of the GDPR 'requires Data Controllers to implement data protection by design and by default' (Art. 29 WP 2017: 8). The example given in this earlier Opinion for how to ensure data protection is designed into systems is the following. When workers are provided with tracking devices, the least privacy-invasive settings should be selected if any monitoring will occur. Not specified in that Article however but of significance relevance is to emphasise that not all tools are identical, obviously, and offer a variety of functions. Various tools and applications have various functions, and products are developed in countries with varying data protection regulation to those required by the GDPR. Therefore, Data Controllers in EU member states (and elsewhere, if companies intend to do business with EU countries), must ensure that software targeted for implementation meets the standards of the GDPR, regardless of where products are designed and manufactured. Then, when legality of the functions available is ensured, Data Controllers, by way of the DPO, should actively and explicitly invite union and other worker representatives to be involved in activities around selecting software and hardware that may be used to monitor and track any aspect of work. Worker representatives should also work with the DPO to negotiate and discuss activities will be tracked and monitored, to agree to and find consensus for legitimacy of these and the

proportionality between business need and workers' rights. If these steps are all met, then a Data Protection Impact Assessment (DPIA) can be carried out. The DPIA also must be carried out with full involvement of worker representatives.

Thus, this first Principle is an overarching Principle, which requires the direct involvement of union representatives in co-decision making; the continuous involvement of worker representative organisations at all stages of the data life cycle in finding consensus for legitimacy and proportionality; playing an active role in co-creation and co-design; and meaningfully involvement in the execution phases of any worker data collection and processing intervention. The Principles and policy options associated, advocate for the insurance of data transparency, meaningful assessment and discernment of legitimacy of practices, aims toward accuracy and worker protection facilitated by checks on practice, and time-boundedness and appropriate storage, which are both monitored and enforceable. Most of the Principles must be both collectively decided and negotiated with unions *before* a DPIA is carried out.

Worker representatives must be appropriately trained with expertise in data protection and work alongside DPOs to ensure these Principles are met. In this way, worker representatives, alongside the DPO can create technical solutions to protect the rights for workers to, for example, explicitly control any device that will monitor their work and associated behaviour, as well as the right to an authentic means to opt out. As stated, where technological tracking is implemented, real opt-out provisions must be built in to systems and hardware which monitor workers, so that workers can decide not to be tracked within the agreements reached with worker organisations. So workers must be both individually and collectively provided with meaningful control over the systems and hardware that monitor their activities. Furthermore, data must not be used for purposes about which workers have not been told and worker representatives agreed via collective bargaining, nor for which it was not originally intended and designed, avoiding function creep.

7.1.2. Proportionality, necessity, transparency

The EDPB's 'Opinion 2/2017 on data processing at work' was published during the first year the GDPR came into force and then became applicable in May 2018, stating that:

> 6.4. Data processing at work must be a *proportionate* response by an employer to the risks it faces taking into account the legitimate privacy and *other interests* of workers. (Art. 29 WP 2017: 23) [italics added by author]

Within 6.4, the identification of workers' *other interests* is mentioned, but in practice, the wider interests of workers and their surrounding rights, are often overlooked. To fully inform 'proportionality', which refers to the proportional necessity for data collection at work balanced between the employer and workers, a range of workers' rights must be taken in to account. Usually, monitoring and tracking are justified with regards to an employer's stated interests, which should be justified in balance and proportion with workers' needs and interests. Proportionality should also take full account of workers' needs and interests, however, as much as a company's or an institution's. Workers' needs are for protection from techno-stress and cyberbullying; shielding from excessive and opaque worker surveillance rather than consented and transparent monitoring and tracking; and the need and right to dignity and personality.

Privacy is more than an interest, it is a right, but there are a whole range of interests surrounding and entangled with aspects of privacy which are at stake and which have relevance for discussions of proportionality, which should be discussed and agreed in meaningful consultations with worker representative groups. For example, during the Covid-19 period, workers have been instructed to work from home, irrespective of the suitability of the home environment for work activities. Where management relied on person to person contact, the question arose, how would work be monitored and performance evaluated given home working? Workers' interests then of course involve privacy,

but other interests are also such as how to accommodate people with caring responsibilities' need for more time away from terminals than others during normal shifts, or the need and indeed, right to a reasonable work/life balance in general to maintain wellbeing as digitalised work seems best suited to infinitely expendable working time schedules.

Precise identification of the seeming *necessity* for technological tracking must be infused with negotiation about what can be deemed proportional to workers' privacy and taking their wider interests seriously. Worker representative organisations must be involved in deciding necessity, proportionality and which workers' interests are at stake every time technological tracking processes are considered in every company and organisation. It is imperative for companies to attempt to identify analogue, non-invasive methods to achieve companies' goals, before seeking to adopt technological tracking and monitoring methods of workers. If there are methods to gain information about workers which do not involve intensive data collecting and processing, those methods should be selected. Indeed, often, technological tracking is simply unnecessary.

Transparency is required by the GDPR, where workers 'must be informed of the existence of any monitoring, the purposes for which personal data are to be processed and any other information necessary to guarantee fair processing' (Art. 29 WP 2017). These requirements are within Art. 13 – 15 of GDPR. In Art. 15.1., data subjects must have access to information about automated decision-making including profiling, and to furthermore be provided with 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' (Hendrickx 2019: 161). This includes the right for incorrect information to be rectified, for incomplete information to be completed, and for workers to gain reports about data being collected, processed and used. This level of transparency is unprecedented in data protection and privacy regulation and is a game-changer in this sphere. However, individual workers must not be laden with the work of gaining and keeping a watch over data. The DPO, unions and worker representatives must actively initiate and sustain communication with workers ensuring these details, allowing workers to engage meaningfully with the process, to have good council on the processes and even to withdraw consent with union assistance. Co-determination is the best way to ensure transparency, proportionality and necessity are sustained and agreed.

7.1.3. Co-determination

Co-determination is where workers sit on management boards and are directly involved in making decisions about working conditions changes and business operations. Most of the EU's post-Brexit members, plus Norway, enjoy some kind of co-determination in state-run firms and the private sector. Those countries which do not enjoy the right to co-determination are Belgium, Bulgaria, Cyprus, Estonia, Italy, Latvia, Lithuania and Romania. Precise rules differ but the process is one that the current report advocates for all EU countries. For example, the German system requires that any time there is a change in worker policy that impacts the speed of work, co-determination is required. Therefore, a company such as Amazon which wants to e.g. implement a time tracking system for workers developing Alexa smart speakers, works councils must be consulted and meaningfully contribute to any change in practice (see Germany's Case Study). This can actually lead to a multinational company implementing varying policies in various subsidiaries across the world, but it means that workers in the German branches may enjoy better working conditions. Successes in co-determination should be considered best practice and companies should require either similar practices or simply implement the resultant policy in all branches. For example, where Amazon has sites in many countries for its product Alexa's natural language processing and other data work activities, if time tracking is not permitted in e.g. the German branch, because a works council has not agreed to it due to the stress and psychosocial problems created for workers, then that type of time tracking should not be allowed in any branch across the world.

Companies must take note of the legal requirements and apparatuses in countries with co-determination rights and implement these in all branches in all countries. Linked to this

recommendation for a company Policy Option, all countries should implement some form of co-determination (also see policy options). In countries where co-determination rights exist, all data collection and processing activity must be co-determined. Where co-determination does not exist, it should become law.

7.1.4. Prevention over detection

Data tracking systems in the health and safety remit should be designed to spot possible problems in advance by ensuring correct procedures are being followed as far as is possible such as CCTV checks at the entrance to construction sites ensuring that workers wear appropriate garments, or in the factory space where robots are used for production, to ensure they are following correct pathways. Prevention is a better approach than solely detecting on-the-spot problems when they arise and then dealing with any aftermath when safety is compromised in these contexts. However, for other identifiers gained from monitoring and tracking that occur in the human resources remit, the concept of 'prevention' is not as straightforward as seen in the construction industry. A justifier for cameras that watch employees in retail has been to prevent thefts (see López Ribalda and Others v Spain). A rationale for introducing backdoors for email and checks on computer usage and so on has been to protect systems from security breaches. However, if there are ways to prevent such activities that do not involve ongoing exposure of a workers' every movement in a store or capture of every stroke to a keyboard conducted by a worker, then the alternative approach should be taken, particularly where the approach does not involve technological tracking. In fact, outright prevention of adoption of technological tracking could at points be a viable option.

7.1.5. Collective data governance

The GDPR is written with the individual as a focal subject. This is similar to the way the 1978 French Law on Freedom and Information Technology portrays the individual citizen and her right to privacy. While this is not wrong, data collection operates at more levels than the discrete and the use of it will impact people individually, as well groups of all kinds, qualities, and quantities.

Some critics have claimed that while the GDPR is written to protect personal data, a lot of data that is collected e.g. on social media is a different type of data, i.e. 'social data' (Benfeldt et al. 2020) which is more often aggregated in the public sphere such as by large social media companies. There are special categories of personal data that are explicitly safeguarded by the GDPR e.g. race and ethnic origin, religious beliefs, political opinions, trade union memberships, biometric, genetic and health data, and data about sexual preferences and sexual orientation. These types of data are important and at the individual level are protected. However, there are a range of inferences about these categories that can be made based on large groupings of data about other characteristics, which should be just as protected against, as the special category of data for individuals, is.

Even where data about individuals is anonymised, machine learning allows a researcher, scientist, or boss, to make judgements about patterns as that data is parceled out. The bigger the dataset, the more powerful it is. Therefore, approaches and responses to data and its collection should not be individualised, such as expected in a consent framework, but should also be collective. Consent is usually perceived to be a unidirectional arrangement and considered intrinsically impossible in the employment relationship. However, in countries which enjoy co-determination rights, digital workspace transformations require negotiation and bargaining between workers and management to proceed. Collective rights are a 'fundamental tool to rationalise and limit the exercise of managerial prerogatives' over individual workers as well as over groups of workers (De Stefano 2019: 41). So, ultimately, the idea of consent must itself be rewritten to allow for workers' data consent, where, because workers cannot automatically provide meaningful consent individually, the idea of a union based, or a kind of collective consent should be considered. Data collection is performed at the collective level and data governance should be seen as a collective good. New ways of thinking about consent can accommodate these expositions.

7.2. Policy options

Workers' interests should always be at the forefront of company approaches to privacy and data protection and worker representatives must always be consulted when a new technology is considered for workplace operations and analytics. Worker representatives' involvement at every increment of the data life cycle of any technological tracking procedure is strongly recommended and involvement in every stage of consideration, design, implementation, and execution, is advised.

7.2.1. Require union/worker involvement at all stages

Worker representative groups must be incorporated into all discussions, design and execution of any data collection, storage, processing and decision-making strategies envisaged and/or incorporated by companies and organisations, alongside the DPO and via membership of company executive and advisory boards. Any organisation with more than 250 employees which processes large sets of data, sensitive data and/or whose central function is to collect and process data; and all public bodies; are required to have a DPO. The role of the DPO and ultimately the Data Controller (the latter of which is normally the organisation or company itself), is to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]. Those measures shall be *reviewed* and *updated* [italics for emphasis] where necessary' (GDPR Art. 24 1., 2).

The role of the DPO can be filled by an already existing employee or partner, but it is advised here that the DPO is provided autonomy and legal protections, since there are times when she or he may face a conflict of interest if they are themselves employed on a regular contract with the same company where she or he works as the DPO. To strengthen the role as one that can appropriately protect worker data subjects, the report suggests that, further to the DPO, a parallel worker representative colleague in the form of a union officer with expertise in data protection rights should be appointed, who will carry out all activities alongside the DPO and who will have as much authority in decision-making as the DPO. This will have particular resonance in countries with co-determination rights. Interestingly, Norway's labour law includes the right to a data shop steward in both the public and private sector in labour law and has done for several years.

Checks must be in place to ensure DPO's responsibilities are met, as outlined in GDPR Art. 39, and audits on whether regular DPIAs are being carried out, where findings should be shared with all parties and even made public, to ensure transparency. These checks should be performed by a third party such as a country's labour authority. While normally, *updates* referred to in Art. 24 1.2 would occur when some modification is made to systems at work involving tracking and monitoring, it is recommended that workers are automatically incrementally approached with explicit offers for the removal of both individual and collective union consent for data collection and processing. Specific tools and methods must be devised to meet GDPR compliance as well as e.g. ECHR Art. 8. If the processes are seen by either employers or workers to have met their goals, to be faulty or to be no longer necessary, they should be modified, re-negotiated, and/or terminated (See Table 2).

But beyond listed requirements in the GDPR, the DPO and unions must be explicitly involved in all stages of all tracking activities, from its first consideration of agreeing proportionality and necessity, to selecting software and hardware, to co-creation and co-design of the packages intended for roll-out with agreed data to be collected and design of the precise systems, schedule and time frame, DPIA and then execution and regular checks as well as updates. Time-boundedness and prevention function creep based on data minimisation must be upheld. DPOs and worker representatives should develop awareness campaigns and training programmes for workers alongside such activities that provide full information about the projects to be executed, and continuous training that provides guidance on data rights.

Table 2 – Collective Determination of Data Rights

Importantly, DPOs are explicitly responsible for taking responsibility for, and for informing data subjects in a transparent manner about the accumulation of personal data and ensuring workers consent to processing and usage of data in most cases. The DPO and their union parallels must meaningfully communicate details of people's rights with regards to that data surrounding access, rectification, erasure, restriction of processing, data portability, notification of explanation in the event of automated decision-making, and must be consulted if the Controller intends to disclose data to third parties (Art. 12, 14). Furthermore, DPOs and related worker representatives must work with human resources to ensure that employment contracts meet GDPR and other privacy and human rights law. Contracts must not contain clauses permitting limitless or unspecified data collection. Employment contracts furthermore must not be separated from data protection contracts.

It is significant to note here that no worker interviewed within the Worker Cameos chapter of the current report believed that they have had meaningful communications with DPOs nor adequate information provided regarding data collection. Where workers gave any kind of consent, it involved ticking a box for access to regular systems and theu were not given any kind of option. Nor were they aware of any withdrawal rights. But explicit corporate-level responsibility is required within the GDPR, where management must discuss data collection activities, meaning that the *worker herself is not ultimately responsible for chasing management* to ensure data protection and privacy law is being kept. Workers should be provided the opportunity to decide whether they consent to personal data collection and use, or not, and the offer of a contract for work should not be contingent on gaining consent except for basics like data needed to accept reimbursement (e.g. bank account details).

DPIAs, introduced in Art. 35 of the GDPR, are required any time a company or organisation wants to collect and process large portions of data and where workers' activities and their communications are directly monitored in all likelihood, due to potential sensitive information that is accumulated:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. (Eur-Lex 2019)

DPIAs should work to prevent excessive monitoring of employees through looking at the risks that may be introduced, consisting of a thorough assessment on whether a data processing system poses a high risk to the rights and freedoms of workers. One of the reports which was prepared by the Art. 29 WP on how to carry out good practices in this arena, and recommends companies gather the following:

> A systematic description of the monitoring, including the scope of the monitoring, the hardware/software used and the period for which the data will be stored.
>
> Details of the necessity and proportionality of the monitoring, including the relevancy of the specific purpose, the level of intrusion into the private sphere of the employee, the potential recipients of the data and details of how the rights of employees will be upheld (e.g. right to access, rectify, erase or limit the portability of the data).

> Details of how the risks to the rights and freedoms of data subjects are managed, including the identification of the sources of risks, the potential impacts and if/ how those risks can be resolved or reduced.
>
> The involvement of interested parties, including not just the relevant employees but the employer's Data Protection Officer (if appointed) and, if any high risks cannot be eliminated, the national data protection authority. (cited in Keane 2018: 361-2)

DPIAs should involve unions in co-authorship and the reports produced should be disseminated both to the entire workforce within that company or organisation, and made publicly available.

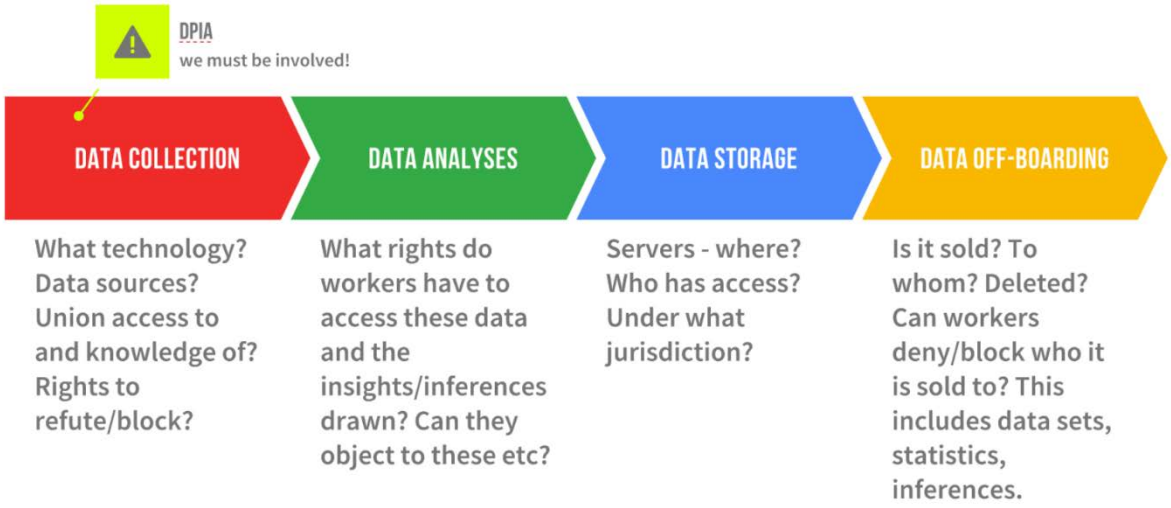
Acknowledging the relatively weak rights which workers in Europe and across the world have in relation to data that is extracted, aggregated and used at work, Dr Christina J. Colclough has prepared a set of recommendations for unions. A Data Lifecycle at Work emphasises full co-governance of 1) data collection, 2) analyses, 3) storage and 4) off-boarding (see Table 3). Workers and employees must be fully informed about all data collected about them, and also participate meaningfully in the full lifecycle of data in these stages. Indeed, Colclough stated, workers have 'a *right* to know'.[6]

Detailed discussions between management and workers about algorithms and data activities that are used in recruitment activities, are rare. Colclough posits that full transparency and knowledge sharing must be part of all worker-data driven corporate activity, regardless of whether work is in the private or public sector. For example, the question of what criteria are included and what is excluded in algorithmic selection should be asked. Colclough also elaborated on the 'right to reasonable inferences' discussed by Wachter and Mittelstadt (2019). Workers can be subject to old and new inferences that have a real life and immediate impact on their work and career paths. For example, a worker can be de-selected for a job due to an algorithmically determined correlation between gender, postcode and performance.

The risk of discrimination is extremely high and the threat to workers' rights large any time algorithmic activities are applied. Colclough emphasised the importance of where data is stored, for how long, and under what jurisdiction. Negotiating this phase will grow in importance if the current e-commerce negotiations in and on the fringes of the WTO are concluded. And finally, workers should have far stronger rights over whether datasets that include their personal data or personally identifiable information are deleted, if so when, or sold, and if so, to whom.

[6] Interview with Christina J. Colclough, expert on the future of work and the politics of digital technologies and the Why Not Lab https://www.thewhynotlab.com/ 26/08/20.

Table 3 – Data Lifecycle @ Work (Colclough 2020)



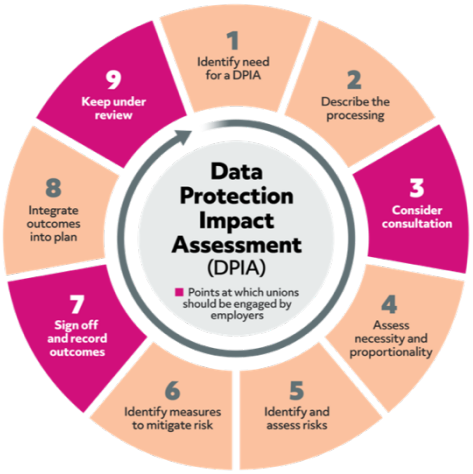
Prospect, a UK trade union that represents 150 000 specialist, technical and engineering, and data driven professionals, is working with the Institute for the Future of Work and the UNI Global Union Federation on a toolkit of data rights intended for wide distribution to unions. The toolkit will include accessible educational materials for non-expert and non-technical worker representatives and union members on existing legislation including the GDPR and a variety of data rights briefings, training materials and events about data rights for workers, and methods to build networks of reps and branches in this arena.

Furthermore, Prospect is in dialogue with the UK ICO about identifying where unions/workers must be involved within the DPIA guidance that the ICO has set out (see Table 4). Prospect's Research Director and Head of Future of Work Andrew Pakes indicated in an interview with Moore that to 'consider consultation' is important, as is emphasised within the ICO's model, but it should move from being a passive concept as it is often treated, to actively engage unions and worker voices at the collective bargaining table and in co-determination wherever possible.[7] Unions should also be involved in any sign-off of DPIAs and outcomes and final drafts agreed. These explicit points of union involvement are designed to ensure that risks arising from worker data collection and processing are identified and mitigated. Pakes stated that 'the GDPR is a building block to enforce transparency' and should be used by unions wherever possible to safeguard rights, and gaps in current guidance identified to push boundaries for workers' rights.[8]

[7] Interview with Andrew Pakes, Prospect Research Director and Head of Future of Work 25/08/20.

[8] Ibid.

Table 4 – Data Protection Impact Assessment (DPIA) – involving unions/workers



Adapted ICO steps for a DPIA (Prospect emphasis on areas for union/worker voice highlighted in pink). (Prospect 2020b)

Keeping unions fully involved in the co-creation, design and execution and at all stages of the data life cycle is intended to flush out the algorithms, their logic, the data they feed on, and the inferences made and designed to lead to a sound co-governance model that will hold management accountable, is responsible and fair, and prevents a growing objectification of workers.

7.2.2. Introduce and enforce co-determination into labour law in all EU member states

Collective bargaining rights and local labour law must be reformed to meet best practices in data protection and privacy for workers, in consultation with trade unions and with cross-border union groups including the International Labour Organization's worker branch, ACTRAV. Co-determination is the best method for all worker bargaining around technological change leading to worker surveillance and all EU countries should adopt some form of it. The German model is particularly strong as it involves co-determination at two levels, at the *Betriebstrat* or shop-floor level, where management is required to consult with and negotiate most changes to working conditions and the working environment with works councils; and the *Aufsichtstrat*, or company level, where workers and their representatives sit on supervisory boards alongside shareholders who work with the executive board. The Chair of the supervisory board holds two votes, and thus can break a tie in negotiation voting.

Steps have been taken already at the international and regional levels to coordinate local negotiations and to deal with struggles arising as digital tracking advances. The UNI Global Union Federation has been very active in responding to digitalisation issues over recent years and published the 'Top 10 Principles for Workers: Data Privacy and Protection' (UNI Global nd). These principles include data processing safeguards, data minimisation, workers' full right to explanation, biometric data exemptions and the recommendations for inter-company data governance bodies as well as collective agreement prioritisation (UNI Global nd). In 2018, 'Trade Union Responses to the Changing World of Work: A report for UNI Global Union' was published (Blakely and Davies 2018) which provides an overview of ways that unions are dealing with the changing digitalised world of work in national contexts. The report acknowledges the overall shape of challenges facing unions at the present moment, including from digitalisation. Indeed, the document acts as something of a 'report back' from various unions on what they have been working on in recent years, sometimes focusing on digital challenges. The entries relating to the digital era and linked in some ways to new monitoring and tracking possibilities of workers include: *GMB* v *Uber* (UK); *Ver.di and platform workers*

(Germany); *Unions NSW* v *Airtasker* (Australia); *Vida, CGIL and NGG* (EU) v *Delivery Hero*; Unites and outsourced IT workers (Nepal); and collective bargaining on digitalisation in Germany, Norway, Netherlands, France and Japan.

Building on the experiences and activities of union partners across the EU and the world, EU states should work to improve national collective bargaining rights and labour law through cross-border discussion and work to agree on best practices via Eurofound, with the emphasis on achieving co-determination rights that should be incorporated in all States. Correspondents from Member States plus Norway regularly report to Eurofound, proposing research questions that inform and establish comparative overviews and identify specific themes for large research projects, which should be about worker data protection and privacy in the GDPR era. Correspondents should also look at the successes from the cases across the EU and reported in the current report. Another good resource is the ILO's Protection of Workers' Personal Data Code of Practice of 1997. An updated framework based on this Code of Practice and good reviews of existing union activities is needed to cultivate cross-border awareness raising as well as the local labour law and trade union coordination.

7.2.3. Businesses to compile certification and codes of conduct

To ensure full inclusion of employers in data tracking and processing activities as partners rather than just directors and managers, all DPOs should be proactive and include not only trade unions but also employer associations. Indeed, to demonstrate good practice, for insurance of lawfulness and workers' rights protections, DPOs should work with employer associations to write codes of conduct to accompany any system processing data. This will ensure that employers understand the wider context within which their activities function and that consultation has operated with a wider employer inclusion. This could even operate at the level of international standards, where, for example, the International Standards Organisation is currently developing a standard that looks at the use of dashboards in such places as warehouses, which takes into account the variety of usages in various countries and the legal frameworks and organisational cultures within which they are operating.

7.2.4. Prioritise collective governance

As indicated in the first principles, the GDPR is oriented around individuals, who are classified as data subjects. Indeed, ECHR Art. 8 secures a range of protections in the individual sense, prioritising the right to both private and family life, home and correspondence, physical, psychological or moral integrity, identity and autonomy, as well as a range of protection for couples, parents, children, and other family relationships (ECtHR 2020). The GDPR is intended to protect *personal* data, but this Policy Option argues that personal cannot be disassociated from the groups and communities within which she or he lives. The family is one grouping, but there are many other kinds of groupings in contemporary life, such as teams of workers in the workplace and workspace. Data collection and privacy therefore must be continuously understood as a set of activities that has implications for groups and therefore, responded to collectively. Along these lines, De Stefano emphasises that 'collective regulation is essential to secure adequate labour protection in times of automation and technologically enhanced monitoring practices' (2019: 41).

Art. 88 of the GDPR stresses that data protection and privacy measures and rules:

> …shall include appropriate and specific measures to preserve the human dignity of data subjects, as well as their legitimate interests and fundamental rights, paying particular attention to the transparency of processing, the transfer of personal data within a business group or a union of undertakings engaged in joint economic activity and workplace supervision systems. (GDPR Art. 88)

The protected classifications of data which are explicitly safeguarded by the GDPR e.g. race and ethnic origin, religious beliefs, political opinions, trade union memberships, biometric, genetic and

health data, and data about sexual preferences and sexual orientation involve individuals. However, aggregate data about these characteristics can and indeed, are used for other purposes. In that way, individual data is turned into group data. Thus, inferences about these categories based on big data, can, and are, made in people analytics for recruitment, hiring, talent management, and so on, as discussed earlier in this report. A collective, or union led response, is necessary and advised here in order to deal collectively with what ultimately, becomes collective data.

Another perhaps more controversial suggestion, is that the idea of consent (see Table 4), which is usually individualised, could be transformed to be understood as something that is not given at the individual, 'tick-box' level, but is done collectively, with union involvement and agreement. GDPR and the E-Privacy Directive (the latter of which has not been finalised at the time of writing), are game-changers for debates around data subject consent, but it is usually considered nigh-impossible to gain meaningful consent from workers. Nonetheless, GDPR Art. 6 lists consent as the first item in the list of ways that a company can achieve lawfulness for data gathering and usage.

Table 4 – Consent

1. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.
2. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.
3. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.
4. Consent should cover all processing activities carried out for the same purpose or purposes.
5. When the processing has multiple purposes, consent should be given for all of them.
6. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. (GDPR recital 32)

GDPR Recital 32 lists requirements which indicate radical new interpretations around how to depict informed consent from data subjects, such as 'silence, pre-ticked boxes or inactivity' which will not constitute consent, as listed in Table 4. While these explicit interventions are promising for the consumer, where for years now, data accumulation has substituted more traditional forms of payment for services, consent is difficult to authentically obtain in the employment relationship due to its inherently imbalanced nature.

The current report recommends, therefore, alongside the EDPB in its 2020 Guidelines 05/2020, that:

> …requirements for consent under the GDPR are not considered to be an "additional obligation", but rather as preconditions for lawful processing. (EDPB 2020: 6)

While consent is only one of six criteria that may be selected by a company to identify lawfulness of actions, consent to data collection and processing is nevertheless worth keeping alive in discussions particularly if co-determination is legislated and during collective bargaining phases of discussion between employers and worker representative groups. Consent could take a different form, intellectually overhauled and reconsidered in definitional terms when discussing unions to be meaningful *if obtained via unions* rather than simply individually.

Where they have chosen this criteria as a way to achieve lawfulness, while a company or organisation may select a method to achieve consent at the individual level, e.g. through written documentation via email, or an oral statement, consent must be accompanied by continuous and regular audits carried out by DPOs, and regularly checked by countries' labour authorities. Technological systems must be regularly reviewed and re-obtained via automatic renewal processes, even without incremental technological changes, as is the current status quo. Meaningful consent must be accompanied by meaningful audits and assurances as well as meaningful moments for workers to reconsider their consent.

8. Conclusion

The global Covid-19 virus pandemic has resulted in yet another upheaval of the labour market and, as people are being asked to work from home, the possibilities for worker tracking are again front and centre. It remains to be seen to what extent electronic monitoring will become increasingly normalised in this context.

This report has, it is hoped, positioned the debates about workers' privacy and data protection rights from a workers' perspective and with a human rights focus; championed the fundamental rights of the European Union Convention on Human Rights; and appealed to the ideals of universal social justice. With a huge amount of generous intellectual assistance from many people, the author of this report has been able to take a frank look at the current state of play in digitalised monitoring and tracking, and data collection and processing. The literature review has oriented debates in the rich history of critical electronic performance, monitoring scholarly writing and policy level wrangling of best ways forward. The country case studies indicate where some countries have been successful in incorporating best practice in providing security for workers as well as turbulence in application of data protection and privacy regulation, where the textured scenarios range from the northern to southern EU countries, to the snowy highlands of Norway, to the busy highways of Nigeria. These orientations are qualified with a series of up to date stories from workers themselves whose experiences with digital monitoring and tracking are variable in many ways, but in two items remain the same: one, where all workers feel the psychosocial strain of work surveillance and two, where no workers felt they were being appropriately informed about what data was being tracked and what aspect of their work was being monitored, nor why.

In this context, the author of the report has provided a set of first principles and policy options that highlight a number of fundamental problems, both in the more abstract purview of legal terminology surrounding protective parameters, and in the practical sense, where companies and organisations are not communicating with workers about digital tracking and data collection transparently. This is fundamentally unacceptable. Therefore, the author has couched her consultation in a set of distinct demarcations for the implementation of the GDPR with a series of worker-focused advances that we hope will work toward an appropriately protected environment for workers' data rights today and into the future.

In conclusion, it is important to keep these debates alive, as these are extremely important times for workers and for management in increasingly unknown environments, where digital tracking and monitoring technologies are part of the everyday experience of people in the new surveillance workplaces and workspaces. The EU is taking this very seriously. It remains to be seen to what extent surveillance in the workplace will continue to expand and what the implications and real life experiences for both positive and other ends, are for workers. The aim of this report is to build on the discussions between policymakers, civil servants, managers, worker representatives, governments, and workers themselves that are already emerging, identifying a series of first principles and policy options based on the literature review and fieldwork outlined above, to guide the imminent future of work, where surveillance, tracking and monitoring are becoming increasingly familiar experiences for workers across industries in the EU, and across the world.

9. References

Aiello, J.R., Svec, C.M. (1993). Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence. Journal of Applied Social Psychology, 23(7), 537-548.

Aiello, J.R., Kolb, K. (1995). Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress. Journal of Applied Psychology, 80(3), 339-353.

Ajana, B. (2018). Metric Culture: Ontologies of Self-Tracking Practices. Bingsley, UK: Emerald.

Ajunwa, I. (2020). The Paradox of Automation as Anti-Bias Intervention, 41 Cardozo, L. Rev. Forthcoming. Available from: https://ssrn.com/abstract=2746078 or http://dx.doi.org/10.2139/ssrn.2746078

Ajunwa, I.; Crawford, K.; Schultz, J. (2017). Limitless Worker Surveillance. California Law Review 105(3), 735-776.

Alder, G. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture Journal of High Technology Management Research, 12, 323- 342.

Alder, G. (2007). Examining the relationship between feedback and performance in a monitored environment: A clarification and extension of feedback intervention theory, Journal of High Technology Management Research, 17, 157-174.

Alder, G., Tompkins, P. (1997). Electronic performance monitoring: An organizational justice and concertive control perspective. Management Communication Quarterly, 10(3), 259-288.

Allen, M., Coopman, S., Hart, J., Walker, K. (2007). Workplace Surveillance and Managing Privacy Boundaries. Management Communication Quarterly - MANAG COMMUN Q. 21. 172-200.

Aloisi, A., Gramano, E. (2019). Artificial Intelligence is watching you at work: Digital surveillance, employee monitoring and regulatory issues in the EU context. Comparative Labour Law and Policy Journal 41(1), 95 – 122. Special Issue 'Automation, Artificial Intelligence and Labour Law', edited by V. De Stefano.

Andrejevic, M. (2005). The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. Surveillance & Society 2(4), 479-497

Arctic Shores (2020). Science. Available from: https://www.arcticshores.com/science/

Areheart, B.A., Roberts, J.L. (2019). GINA, Big Data, and the Future of Employee Privacy. Yale Law Journal 128(3), 710-790.

Ariss, S., Nykodym, N., Cole-Laramore, A.A. (2002). Trust and Technology in the Virtual Organization. SAM Advanced Management Journal, 67(4), 22-25.

Atteslander, P.M. (2008). Methoden der empirischen Sozialforschung. Berlin: Schmidt, Erich Verlag.

Bain, P. and Taylor, P. (2000). Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. New Technology, Work and Employment, 15(1), 2–18.

Ball, K. (2010). Workplace surveillance: an overview, Labour History, 51(1), 87-106

Ball, K. (2014). The Harms of Electronic Surveillance in the Workplace. Available from: https://pen.org/the-harms-of-electronic-surveillance-in-the-workplace/

Ball, K. and Margulis, S. T. (2011). Electronic Monitoring and Surveillance in Call Centres: A Framework New Technology, Work and Employment, 26(2), 113 – 126.

Ball, K. and Wood, M. D. (2006). A report on the Surveillance Society for the United Kingdom Information Commissioner. Available from:

https://webcache.googleusercontent.com/search?q=cache:0kYWgfG29pMJ:https://ico.org.uk/media/about-the-ico/documents/1042391/surveillance-society-summary-06.pdf+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b-d

Barley, S. and Kunda, G. (1992). Design and Devotion: Surges of Rational and Normative Ideologies of Control in Managerial Discourse. Administrative Science Quarterly 37(3), 363-300.

Baumann, Z. and Lyon, D. (2012). Liquid Surveillance: A Conversation. Cambridge: Polity Press.

BBC (2019). Is your boss watching you? In the Balance. Available from: https://www.bbc.co.uk/programmes/w3csy9v4

Beer, D. (2017). The social power of algorithms. Information, Communication & Society 20(1), 1-13.

Bélanger, J. & Thuderoz, C. (2010). The Repertoire of Employee Opposition In Smith C. (ed.), Working Life: Renewing Labour Process Analysis. Critical Perspectives on Work and Employment. London: Palgrave Macmillan.

Benfeldt, O., Stouby Persson, J. and Madsen, S. (2020). Data Governance as a Collective Action Problem. Information Systems Frontiers 22, 299 – 313.

Berg, J. (2016). Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers. Conditions of Work and Employment Series No 74, Geneva: International Labour Organization.

Berg, J., De Stefano, V. (2017). It's time to regulate the gig economy. Open Democracy. Available from: https://www.opendemocracy.net/beyondslavery/janine-berg-valerio-de-stefano/gig/it-s-time-to-regulate-gig-economy

Berinato, S. (2015). Corporate Wellness Programs Make Us Unwell: An Interview with André Spicer. Harvard Business Review, 28–29. Available from: https://monthlyreview.org/2019/02/01/new-means-of-workplace-surveillance/#en74backlink

Bersin, J., Mariani, J., Monahan, K. (2016). Will IoT Technology Bring us The Quantified Employee? The Internet of Things in Human Resources. Deloitte University Press. Available from: http://dupress.com/articles/people-analytics-internet-of-things-iot-human-resources/#end-notes

Betterworks (2019). Homepage. Available from: https://www.betterworks.com/product/goals/

Blakely, H., Davies, S. (2018). Trade Union Responses to the Changing World of Work: A report for UNI Global Union. Nyon, Switzerland: UNI Global Union.

Bloom, P. (2019). Monitored: Business and Surveillance in a Time of Big Data. London: Pluto Press.

Boewe, J., Schulten, J. (2017). The Long Struggle of the Amazon Employees: Laboratory of Resistance: Interim Assessment and Prospects for Union Organising at the Global E-Commerce Leader in Germany and Europe. Brussels: Rosa-Luxemburg-Stiftung.

Booth, A., Sutton, A., and Papaioannou, D. (2016). Systematic Approaches to a Successful Literature Review. London: Sage.

Borgesius, F. Z. (2018). Discrimination, artificial intelligence and algorithmic decision-making. Strasbourg: Council of Europe.

Brady, T. M. (2018). Wrist band haptic feedback system, US 2017/0278052 A1.

Brawley, A.M.; Pury, C.L.S. (2016). Work experiences on MTurk: Job satisfaction, turnover, and information sharing. Computers in Human Behavior, 54, 531–546.

Briziarelli, M., Armano, E. (2020). The Social Production of Radical Space: Machinic Labour Struggles Against Digital Spatial Abstractions. In Moore, P. V., Briken, K., Engster, F. (eds.). Machines & Measure,

Special Issue of Capital & Class. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478542

Brod, C. (1982). Managing Technostress: Optimising the Use of Computer Technology. The Personnel Journal, 61(10), 753 – 757.

Bronowicka, J., Ivanova, M., Klicki, W., King, S., Kocher, E., Kubisa, J., Zielińska, J. (2020). 'Game That You Can't Win'? Workplace Surveillance in Germany and Poland. Frankfurt (Oder): European University Viadrina.

Brown, I. (2020). The Technical Components of Interoperability as a Tool for Competition Regulation. OSF Preprints. 09/10/20. Available from: doi:10.31219/osf.io/6er3p.

Brown, T. (2009) The Gig Economy. Daily Beast 12/01/09, updated 14/07/17. Available from: https://www.thedailybeast.com/the-gig-economy

Business, Innovation and Skills (BIS) Committee (2016). The Digital Economy. London: House of Commons.

Carey, C. S. (2018). Letter to Barbara Elizabeth Duvall, 4 September. Published by The Verge 25/4/19. Available from: https://cdn.vox-cdn.com/uploads/chorus_asset/file/16190209/amazon_terminations_documents.pdf

Cederström, C., Spicer, A. (2015). The Wellness Syndrome. Cambridge: Polity Press.

Cherry, M. A. (2016). People analytics and invisible labour. Saint Louis University Law Journal. 61(1), 1-16.

Clarke, R. (1987). Information Technologies and Dataveillance. Communications of the Association for Computing Machinery 31(5), 498-512

Codagnone, C., Biagi, F., Abadie, F. (2016). The Future of Work in the 'Sharing Economy': Market Efficiency and Equitable Opportunities or Unfair Precarisation?, Institute for Prospective Technological Studies, JRC Science for Policy report EUR 27913 EN, doi:10.2791/431485. European Commission, Brussels.

Cohen, J. (2013). What Privacy is For, Harvard Law Review, 126, 1904-32.

Cohen, J. (2015). The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In Barney, D., Coleman, G., Ross, C., Sterne, J. & Tembeck, T. eds., The Participatory Condition. Minnesota, USA: University of Minnesota Press.

Cohn, J. E. (2017). Ultrasonic bracelet and receiver for detecting position in 2D plane, US 2017/0278051 A1.

Collins, L., Fineman, D. R., Tshuchica, A. (2017). People analytics: Recalculating the route. Deloitte Insights. Available from: https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2017/people-analytics-in-hr.html

Colman, F., Bühlmann, V., O'Donnell, A., van der Tuin, I. (2018). Ethics of Coding: A report on the Algorithmic Condition [EoC]. H2020-EU.2.1.1. – INDUSTRIAL LEADERSHIP – Leadership in enabling and industrial technologies – Information and Communication Technologies, 1–54. Brussels: European Commission. 732407. Available from: https://cordis.europa.eu/project/rcn/207025_en.html.

Corbin, J., Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory (3rd ed.). London: Sage Publications, Inc.

Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. Big Data & Society 3(1), 1-6.

Custers, B., Ursic, H. (2018). Worker privacy in a Digitalised World under European Law. Comparative Labour Law & Policy Journal, 39(2), 323 - 344.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters Business News. Available from: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Data Protection Working Party (Art. 29 WP) (2017). Opinion 2/2017 on data processing at work. Adopted on 8 June 2017 17/EN WP 249. Available from: https://webcache.googleusercontent.com/search?q=cache:tTjbSGQErMoJ:https://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D45631+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b-d.

Deleuze, G. (1990). Post-scriptum sur les societies de controle [Post-script on the Societies of Control], in Pourparlers 1972 - 1990, 240 – 244. Paris: Les éditions de Miuit.

Delponte, L. (2018). European Artificial Intelligence leadership, the path for an integrated vision. Brussels, Policy department for Economic, Scientific and Quality of Life Policies, European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf.

De Stefano, V. (2019). 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Comparative Labour Law & Policy Journal 41(1), 15 - 46.

Directive 95/46/EC (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

Directorate General of Human Rights and Rule of Law (2019). Guidelines on Artificial Intelligence and Data Protection. Available from: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8.

Donovan, S.A., Bradley, D.H., Shimabukuro, J.O. (2016). What does the gig economy mean for workers? Washington, DC: Congressional Research Service.

Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. Big Data & Society 3(2), 1-11.

Duhigg, C. (2019). Is Amazon Stoppable? New Yorker 10/10/19. Available from: https://www.newyorker.com/magazine/2019/10/21/is-amazon-unstoppable

Edwards, P. (2003). The Employment Relationship and the Field of Industrial Relations. In: Industrial Relations: Theory and Practice in Britain (2nd Edition). Malden, MA: Blackwell Publishing.

Edwards, L., Veale, M. (2017). Slave to the Algorithm? Why a 'Right to an Explanation' is Probably not the Remedy you are Looking For. 16 Duke Law & Technology Review, 18-84.

Edwards, L., Martin, L. and Henderson, T. (2018). Employee Surveillance: The Road to Surveillance is Paved with Good Intentions. Available from: https://ssrn.com/abstract=3234382 or http://dx.doi.org/10.2139/ssrn.3234382

Ernst, E.; Merola, R.; Samaan, D. (2018). The economics of artificial intelligence: Implications for the future of work. ILO Future of Work Research Paper Series. Geneva: International Labour Office. Available from: https://www.ilo.org/global/topics/future-of-work/publications/research-papers/WCMS_647306/lang--en/index.htm

Eur-Lex Access to European Union Law (2019). Document 32016R0679. Available from: https://eur-lex.europa.eu/legal content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

European Commission (EC) (nd). Article 29 Working Party Archives 1997 – 2016. Available from: https://ec.europa.eu/justice/article-29/documentation/index_en.htm

European Commission (2018). Communication on Artificial Intelligence for Europe. Brussels, European Commission. Available from: https://webcache.googleusercontent.com/search?q=cache:Z8V8-ollFkAJ:https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF+&cd=2&hl=en&ct=clnk&gl=uk&client=firefox-b-d

European Commission (2020). On Artificial Intelligence. A European approach to excellence and trust. White Paper. Available from:

https://webcache.googleusercontent.com/search?q=cache:VR6rVqV3V_4J:https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b-d

European Court of Human Rights (ECtHR) (2016). Case of Bărbulescu V Romania, App. 61496/08 Judgements (Merits and Just Satisfaction) 12/01/2016 Legal Summary. Available from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}

ECtHR (2020). Guide on Article 8 of the European Convention on Human Rights. Available from: https://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis/guides&c=

European Data Protection Board (EDPB) (2020). Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. Adopted on May 2020.

European Parliament (2017). Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics. Available from: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html

Erwin, S. (2015). Living by Algorithm: Smart Surveillance and the Society of Control, Humanities and Technology Review, 34, 28-69.

Fairweather, B. (1999). Surveillance in employment: The case of teleworking. Journal of Business Ethics 22 (1), 39-49.

Farr, C. (2016). How Fitbit Became the Next Big Thing in Corporate Wellness. FastCompany 04/18/16. Available from: https://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness

FitBit Health Solutions (2019). Homepage. Available from: https://healthsolutions.fitbit.com/

Felstead, A., Jewson, N., Phizacklea, A., Walters, S. (2002a). The option to work at home: another privilege for the favoured few?'. New Technology, Work and Employment 17(3), 204-223.

Felstead, A., Jewson, N., Phizacklea, A., Walters, S. (2002b). Opportunity to work at home in the context of work-life balance. Human Resource Management Journal 12(1), 54-76.

Foucault, M. (2007). Security, Territory, Population: Lectures at the College de France, 1977 – 1978. London: Palgrave Macmillan.

Gandini, A. (2018). Labour process theory and the gig economy. Human Relations. Available from: https://doi.org/10.1177/0018726718790002

Gandy, O. (1993). The panoptic sort: a political economy of personal information. Boulder: Westwiew Press.

GDPR Enforcement Tracker (2020). Available from: https://www.enforcementtracker.com/

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation and the hidden decisions that shape social medial. USA: Yale University Press.

Glockner, H., Jannek, K., Mahn, J., Theis, B. (2014). DHL Research Augmented Reality in Logistics: Changing the way we see logistics – a DHL perspective. Troisdorf: DHL.

Graham, M.; Hjorth, I.; Lehdonvirta, V. (2017). Digital labour and development: Impacts of global digital labour platforms and the gig economy on worker livelihoods. Transfer: European Review of Labour and Research 23(2), 135–162.

Graham, M.; Lehdonvirta, V., Wood, A.; Barnard, H.; Hjorth, I.; Simon, D. P. (2017). The risks and rewards of online gig work at the global margins. Oxford, Oxford Internet Institute. Available from: https://www.oii.ox.ac.uk/publications/gigwork.pdf

Graham, S., Wood, D. (2003). Digitizing surveillance: categorization, space and inequality. Critical Social Policy, 20(2), 227-248.

Grandview Research (2020). Corporate Wellness Market Worth $97.4 Billion By 2027. Available from: https://www.grandviewresearch.com/press-release/global-corporate-wellness-market

Grant, R. and Higgins, C. (1989). Monitoring Service Workers via computer: The effect on employees, productivity and service'. National Productivity Review 8(2), 101 – 112.

Grant, R. A., Higgins, C. A., & Irving, R. H. (1988). Computerized Performance Monitors: Are They Costing You Customers? Sloan Management Review, 29(3), 39-45.

Gray, M. L., Suri, S. (2019). Ghost Work: How to Stop Silicon Valley from building a New Global Underclass. New York: Mariner.

Gregg, M. (2011). Work's Intimacy. London: Polity.

Griffith. T. L. (1993). Monitoring and Performance: A comparison of Computer and Supervisor Monitoring. Journal of Applied Social Psychology, 23, 549-572.

Hitlin, P. (2016). Research in the Crowdsourcing Age: A case study. Washington, DC, Pew Research Centre. Available from: http://www.pewinternet.org/2016/07/11/research-in-the-crowdsourcing-age-a-case-study/

Henderson, R., Mahar, D., Saliba, A., Deane, F., & Napier, R. (1998). Electronic monitoring systems: an examination of physiological activity and task performance within a simulated keystroke security and electronic performance monitoring system. International Journal of Human–Computer Studies, 48, 143–157.

Hoare, K. J., Mills, J., Francis, K. (2012). Dancing with data: An example of acquiring theoretical sensitivity in a grounded theory study. International Journal of Nursing Practice 18, 240 - 245.

Home Office UK (2018). Explanatory Memorandum to the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record Keeping Purposes) Regulations 2018, paragraph 7.4. Available from:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/669129/Investigatory_Powers__Interception_by_Businesses_etc__for_Monitoring_and_Record-Keeping_Purposes__Regulations_2018_-_EM.pdf

Houghton, E., Green, M. (2018). People analytics: Driving business performance with people data, Chartered Institute for Personnel Development (CIPD). Available from: https://www.cipd.co.uk/knowledge/strategy/analytics/people-data-driving-performance

Humanyze (2020). Corporate website. Available from: https://www.humanyze.com/about/

IBM (2018). IBM Talent Business Uses AI to Rethink The Modern Workforce. IBM Newsroom. Available from: https://newsroom.ibm.com/2018-11-28-IBM-Talent-Business-Uses-AI-To-Rethink-The-Modern-Workforce

Information Commissioner's Office (ICO) (2013a). Data Protection. The Employment Practices Code. Supplementary Guidance. Available from: https://ico.org.uk/media/for-organisations/documents/l66/employment_practice_code_supplementary_guidance.pdf

ICO (2013b). In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information. Available from: https://ico.org.uk/media/1542/cctvcode-of-practice.pdf

ICO (2019). Rights related to automated decision making including profiling. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

Irish Data Protection Commission (2019). Data Protection Statement. Available from: https://www.dataprotection.ie/en/about-our-site/data-protection-statement

Jeffrey, M. (2002). Information Technology and workers' privacy: the English law. Comparative Labour Law & Policy Journal 23(1), 301-349.

Jervis, C.E.M. (2018). Bărbulescu V Romania: Why There is no Room for complacency when it comes to privacy rights in the workplace. Industrial Law Journal 47(3), 440-453.

Joinson, A. N. (2008). Looking at, Looking up or Keeping up with People? Motives and Use of Facebook. Proceedings of the Twenty-sixth Annual SIGCHI Conference on Human Factors in Computing Systems, April 5-10 2008 Florence (Italy), 1027 – 1036.

Judd, C. H. (1905). Practice without knowledge of results. Psychological Review Monographs, 2(7, suppl.), 185–198.

Kaplan, E. (2015). The Spy Who Fired Me: The Human Costs of Workplace Monitoring. Harper's magazine 31 (Mar. 2015). Available from: http://www.populardemocracy.org/sites/default/files/HarpersMagazine-2015-03-0085373.pdf [https://perma.cc/5RC3-HK8A].

Keane, E. (2018). The GDPR and Employee's Privacy: Much Ado but Nothing New. King's Law Journal, 29(3), 354-363.

Kenney, M., Zysman, J. (2016). The rise of the platform economy. Issues in Science and Technology, 32(3). Available from: http://issues.org/32-3/the-rise-of-the-platform-economy/#comments

Kent, R. (2018). Social Media and Self-Tracking: Representing the 'Health Self'. In: Self-Tracking: Empirical and Philosophical Investigations. Ajana, B. (ed.). Switzerland: Springer/Palgrave, 61 - 76.

Kizza, J., & Ssanyu, J. (2005). Workplace surveillance. In J. Weckert, J. (ed.), Electronic monitoring in the workplace. Controversies and solutions. London: Idea Group Publishing, 1-18.

Kohll, A. (2016). 8 Things You Need to Know about Employee Wellness Programs. Forbes 21/04/16 Available from: http://www.forbes.com/sites/alankohll/2016/04/21/8-things-you-need-to-know-about-employee-wellness-programs/#1ec78c4d610c

Kravets, D. (2015). Worker fired for disabling GPS app that tracked her 24 hours a day. Ars Technica 05/11/15. Available from: https://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/

Lampe, C., Ellison, N. and Steinfield, C. (2006). A Face(book) in the Crowd: Social Searching vs. Social Browsing. In Proceedings of the 2006 20th Anniversary Conference on Computer-Supported Cooperative Work (CSCW 2006), 167-170. New York, NE: ACM Pres.

Lecher, C. (2019). How Amazon automatically tracks and fires warehouse workers for 'productivity'. The Verge 25/04/19. Available from: https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

Levy, K.E.C. (2015). The contexts of control: Information, power, and truck-driving work. The Information Society, 31:2, 160-174, DOI: 10.1080/01972243.2015.998105

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. Journal of Organizational Behaviour, 23(5), 675–694.

Lugaresi, N. (2010). Electronic privacy in the workplace: transparency and responsibility. International Review of Law, Computers and Technology, 24(2), 163-73.

Lupton, D. (2012). M-Health and Health Promotion: The Digital Cyborg and Surveillance Society. Social Theory & Health 10(3), 229 - 244.

Lupton, D. (2013). Understanding the Human Machine. IEEE Technology and Society Magazine Winter, 23.

Lupton D. (2017). Feeling your data: Touch and making sense of personal digital data, New Media and Society 19, 1599 - 1614.

Lyon, D. (1994). The Electronic Eye. The Rise of Surveillance Society. Cambridge: Polity Press.

Madan, U., Bundy, M. E., Glick, D. D., Darrow, J. E. (2018). Augmented reality user interface facilitating fulfilment. US 2018/0218218 A1.

Market Research Future (2019). Employee Monitoring Software Industry Trends. Available from: https://www.worktime.com/2019-employee-monitoring-software-industry-trends

Marx, G.T. (1992). Let's Eavesdrop on Managers 20/04/92. Computerworld, 29.

Marx, G.T. (1988). Undercover: Police Surveillance in America. Berkeley: University of California Press.

Marx, G.T. (2002). What's New about the 'New Surveillance'? Classifying for Change and Continuity. Surveillance & Society 1(1), 9– 29.

Marx, G.T. (2005). Surveillance and Society Encyclopedia of Social Theory. Available from: http://web.mit.edu/gtmarx/www/surandsoc.html

Marvin, R. (2019). The Best Employee Monitoring Software for 2019. PC Magazine 27/09/19. Available from: https://uk.pcmag.com/cloud-services/92098/the-best-employee-monitoring-software

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited, Theoretical criminology: An international journal, 1(2), 215-232.

Moore, P. V. (2018a). Tracking affective labour for agility in the quantified workplace. Body & Society 24(3), 39-67.

Moore, P. V. (2018b). The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work. Geneva: International Labour Organization, ACTRAV.

Moore, P. V. (2018c). The quantified self in precarity: Work, technology and what counts. London: Routledge.

Moore, P. V. (2019). OSH and the future of work: Benefits & risks of artificial intelligence tools in workplaces. European Union Agency for Safety and Health at Work (EU-OSHA) Focal Point Expert report, Bilbao: EU-OSHA. Available from: https://osha.europa.eu/en/publications/osh-and-future-work-benefits-and-risks-artificial-intelligence-tools-workplaces/view

Moore, P. V. (2020a). The mirror for (artificial) intelligence: In whose reflection? Special Issue, Automation, AI, and Labour Protection. Ed. by Prof Valerio de Stefano, Comparative Labour Law and Policy Journal, 41(1), 47 - 67.

Moore, P. V. (2020b). Kunstliche Intelligenz und 'smarte' arbeit. Rosa Luxemburg Stiftung Brussels, Berlin. 08.2020. Available from: https://www.rosalux.de/profil/es_detail/L8G8NDCHC8/phoebe-moore

Moore, P. V., Joyce, S. (2020). Black box or hidden abode? The expansion and exposure of platform work management. Review of International Political Economy, 27(3), 926 – 948.

Moorman, R. H., Wells, D. L. (2003). Can electronic performance monitoring be fair? Exploring relationships among monitoring characteristics, perceived fairness, and job performance. Journal of Leadership and Organizational Studies 10(2), 2 – 16.

Motorola (2008). WT4000 series wearable terminal specification sheet. Available from: https://cdn.barcodesinc.com/themes/barcodesinc/pdf/Motorola/wt4090.pdf

Motorola (2009). MC3000 Family Specification Sheet. Available from: https://cdn.barcodesinc.com/themes/barcodesinc/pdf/Motorola/mc3000.pdf

Mujtaba, B. G. (2003). Ethical implications of employee monitoring: What leaders should consider. Journal of Applied Management and Entrepreneurship, 8, 22-47.

Nebeker, D. (1987). Automated Monitoring, Feedback and Rewards: Effect on Workstation Operator's Performance, Satisfaction and Stress, in H. Bullinger and B. Shackel (eds), HCI Interact '87, Amsterdam: Elsevier, 833–837.

Nebeker, D.,Tatum, B. (1993). The Effects of Computer Monitoring, Standards and Rewards on Work Performance, Job Satisfaction and Stress. Journal of Applied Social Psychology 23, 508–536.

Newton, C. (2019a). Bodies in Seats. The Verge. Available from: https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa

Newton, C. (2019b). The Trauma Floor: The secret lives of Facebook moderators in America. The Verge. Available from: https://www.getrevue.co/profile/caseynewton/issues/coronavirus-and-the-emergency-in-content-moderation-233920

Nield, D. (2014). In corporate wellness programs, wearables take a step forward. Fortune 15 Apr. 2014. Available from: http://fortune.com/2014/04/15/in-corporate-wellness-programs-wearables-take-a-step-forward/

Noble, S. A. (2018). Algorithms of oppression: How search engines reinforce racism. New York: New York University Press.

Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. Labour and Law Issues 3(2), 2421-2695.

O'Neil, C. (2016). Weapons of maths destruction. New York: Crown Publishers.

Organisation for Economic Cooperation and Development (OECD) (2019). Recommendation of the Council on Artificial Intelligence, OECD, LEGAL/0449 (May 12, 2019). Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Otto, M. (2015). The right to privacy in employment: in search of the European model of Protection. European Labour Law Journal 6, 343 – 363.

Plan C (2017). Creatures of the Night: Changes in the Labour Process at Sainsbury's. 22 March. Available from: https://www.weareplanc.org/blog/creatures-of-the-night-changes-in-the-labour-process-at-sainsburys/

Poster, M. (1990). The mode of information: poststructuralism and context. Chicago: University of Chicago Press.

Poster, W. R. (2011). Emotion Detectors Answering Machines and E-Unions: Multi-Surveillance in the Global Interactive Service Industry. American Behavioral Scientist, 55(7), 868-901.

Poster, W. R. (2018). Close Watch of a Distant Manager: Multisurveillance by Transnational Clients in Indian Call Centres in Moore, P.V., Upchurch, M. and Whittaker, X. (eds.) *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*. Switzerland: Palgrave Macmillan, 151-180.

Power, B. (2016). Why John Deere Measures Employee Morale Every Two Weeks. Harvard Business Review 24/05/16. Available from: https://hbr.org/2016/05/why-john-deere-measures-employee-morale-every-two-weeks

Prassl, J. (2018). Humans as a Service: The Promise and Perils of Work in the Gig Economy. Oxford: Oxford University Press.

Price Waterhouse Cooper (PwC) (2018). AI will create as many jobs as it displaces by boosting economic growth. Online: https://www.pwc.co.uk/press-room/press-releases/AI-will-create-as-many-jobs-as-it-displaces-by-boosting-economic-growth.html

Prospect (2020a). Future of work, technology and data. Available from: https://prospect.org.uk/about/future-of-work-technology-and-data/

Prospect (2020b). Negotiating on data rights. Unpublished.

Purdy, M., Zealley, J., Maseli, O. (2019). The Risks of Using AI to Interpret Human Emotions. Harvard Business Review 18/11/19. Available from: https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions

Reinhard, H.J. (2002). Information technology and workers' privacy: Enforcement. Comparative Labour Law & Policy Journal, 23, 527-531.

Roberts, S. T. (2019). Behind the Screen: Content Moderation in the Shadows of Social Media. USA: Yale University Press.

Rosenblat, A., Stark, L. (2016). Algorithmic labour and information Asymmetries: A Case Study of Uber's Drivers. International Journal of Communication 10, 3758 – 3784.

Rosenblat, A., Kneese, T., Boyd, D. (2014). Workplace Surveillance. Open Society Foundations. Future of Work Commissioned Research Papers. Available from: https://ssrn.com/abstract=2536605 or http://dx.doi.org/10.2139/ssrn.2536605

Rosengren, C., Ottosson, M. (2016). Employee monitoring in a digital context. In Daniels, J., Gregory, K., McMillan Cottom, T. (eds.), Digital sociologies. Policy Press, 181-194.

Ross, S. (1992). Big Brother in Workplace Growing Bigger Every Day. Reuter Business report 15/09/92, pp. 11-12.

Salancik, G. R., Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. Administrative Science Quarterly, 23, 223–253.

Sánchez-Monedero, J., Dencik, L., Edwards, L. (2019). What Does It Mean to 'Solve' the Problem of Discrimination in Hiring? Available from: https://ssrn.com/abstract=3463141 or http://dx.doi.org/10.2139/ssrn.3463141

Sanders, A. L. (1990). Reach Out and Tape Someone. 08/01/90. Time, 55.

Sarpong, S., Rees, D. (2014). European Management Journal Assessing the effects of 'big brother' in a workplace: The case of WAST. European Management Journal, 32(2), 216-222.

Savage, M. (2018). Thousands Of Swedes Are Inserting Microchips Under Their Skin (October 22, 2018) USA National Public Radio (NPR). Available from: https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin?t=1575032564092

Schumacher, S. (2010). What Employees Should Know About Electronic Performance Monitoring. ESS AI : Vol. 8, Article 38. Available from: http://dc.cod.edu/essai/vol8/iss1/38

Schwartz, O. (2019). The rise of microchipping: are we ready for technology to get under the skin? Guardian 08/11/19. Available from: https://www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin

Seaver, N. (2018). What should an anthropology of algorithms do? Cultural Anthropology, 33(3), 375-385.

Sewell, G. (1998). The discipline of teams: the control of team-based industrial work through electronic and peer surveillance. Administrative Science Quarterly, 43, 406-469.

Sewell, G. (2005). Nice work? Rethinking managerial control in an era of knowledge work 12. Organization, 12(5), 685-704.

Sewell, G., Barker, J. (2006). Coercion versus Care: Using Irony to Make Sense of Organizational Surveillance. The Academy of Management Review, 31(4), 934-961. Available from: http://www.jstor.org/stable/20159259

Sewell, G., Barker, J. R., Nyberg, D. (2011). Working under intensive surveillance: When does measuring everything that moves become intolerable? Human Relations, 65(2), 189 – 215.

Siegel, J., Dubrovsky, V., Keisler, S., McGuire, T. W. (1986). Group processes in computer-mediated communication. Organizational Behavior and Human Decision Processes, 37, 157–187.

Silberman, M., Johnston, H. (2020). Using GDPR to improve legal clarity and working conditions on digital labour platforms' European Trade Union Institute (ETUI) Working Paper 2020.05. Available from: https://www.etui.org/publications/using-gdpr-improve-legal-clarity-and-working-conditions-digital-labour-platforms

Smith, W.P., Tabak, F. (2009). Monitoring Employee E-mails: Is There Any Room for Privacy?, Academy of Management Perspectives, 23 (4), 33-48.

Srnicek, N. (2017). Platform Capitalism. Bristol: Polity Press.

Stanton, J. (2000). Reactions to Employee Performance Monitoring: Framework, Review and Research Directions, Human Performance 13(1), 85-113.

Stanton, J., Barnes- Farrell, J. (1996). Effects of Electronic Performance Monitoring on Personal Control, Task Satisfaction, and Task Performance Journal of Applied Psychology, 81(6), 738-745.

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

Staples, W. G. (2014). Everyday Surveillance: Vigilance and Visibility in Postmodern Life. United Kingdom: Rowman and Littlefield.

Stevens, A., Lavin, D. (2007). Stealing Time: The Temporal Regulation of Labour in Neoliberal and Post-Fordist Work Regime. Democratic Communiqué, 21(2).

Strauss, A., Corbin, J. (1990). Basics of Qualitative Research. Newbury Park, CA: Sage Publications.

SupplyChainDigest (2018). Amazon Files Patent for Augmented Reality Putaway, Critics Again Erroneously Worry about Big Brother. SupplyChainDigest. Available from: http://www.scdigest.com/ontarget/18-08-06-1.php?cid=14531

Taylor, F. W. (1911). The Principles of Scientific Management. New York: Harper & Bros.

Taylor, M. (via BEIS Committee) (2017). Good Work: The Taylor Review of Modern Working Practices, London. Available from: https://www.gov.uk/government/publications/good-work-the-taylor-review-of-modern-working-practices

The Economist (2009). Big Brother Bosses. Economist 392.8648 71-72. Business Source Elite. EBSCO. Web. 18/11/2018 Available from: https://www.economist.com/business/2009/09/10/big-brother-bosses

Thompson, P. (2003). Fantasy Island: A labour process critique of the 'age of surveillance'. Surveillance & Society 1 (2), 138–151.

Thompson, P., McDonald, P., O'Connor, P. (2019). Employee Dissent on Social Media and Organisational Discipline. Human Relations. Online first DOI: https://doi.org/10.1177/0018726719846262

Till, C. (2019). Creating automatic subjects: Corporate wellness and self-tracking. Health: An Interdisciplinary Journal for the Social Study of Health, Illness and Medicine 23(4), 418-435.

Tokunaga, S. (2011). Social Networking Site or Social Surveillance Site? Understanding the Use of Interpersonal Electronic Surveillance in Romantic Relationships. Computers in Human Behaviour 27(2), 705-713.

Trades Union Congress (TUC) (2018). I'll be watching you: A report on workplace monitoring. Congress House, London: TUC. Available from: https://www.tuc.org.uk/research-analysis/reports/ill-be-watching-you

Tribunal Constitucional de España (2013). Sentencia 29/2013, 11 de febrero. Available from: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/23284

Tucker, C. (2019). Privacy, Algorithms, and Artificial intelligence. In Agarwal, A. Gans, J. and Goldfarb, A. (eds.). The Economics of Artificial Intelligence: An Agenda. National Bureau of Economic Research. Chicago and London: The University of Chicago Press, 423 – 438.

United Kingdom Department for Business, Energy and Industrial Strategy and Department for Digital, Culture, Media and Sport (2018). AI Sector Deal Policy Paper. Available from: https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

UNI Global Union (nd). Top 10 Principles for Workers: Data Privacy and Protection. Available from: http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf

United States Congress (1987). The Electronic Supervisor: New Technology, New Tensions. Washington, DC: Office of Technology Assessment, US Government Printing Office.

Varca, P. (2006). Telephone Surveillance in Call Centres: Prescriptions for Reducing Strain. Managing Service Quality, 2, 290–305.

Vigneau, C. (2002). Information Technology and Workers' Privacy: The French Law. Comparative Labour Law and Policy Journal, 23(4), 351-376

Wachter, S., Mittelstadt, B. (2019). A Right to Reasonable Inferences. Columbia Business Law Review. 2, 494–620.

Wajcman, J. (2015). Pressed for Time: The Acceleration of Life in Digital Capitalism. Chicago: University of Chicago Press.

Wallach, S. (2011). The Medusa Stare: surveillance and monitoring of employees and the right to privacy. International Journal of Comparative Labour Law and Industrial Relations, 27(2), 189-219.

Waters, F., Woodcock, J. (2017). Far from seamless: A workers' inquiry at Deliveroo. *Viewpoint Magazine*, 20/09/17. Available from: https://www.viewpointmag.com/2017/09/20/far-seamless-workers-inquiry-deliveroo/

Weizenbaum, J. (1972). On the Impact of the Computer on Society: How does one insult a machine? Science 176, 609 – 176.

White House Office of Science and Technology Policy (2018). Summit on Artificial Intelligence for American Industry. Available from: https://www.whitehouse.gov/articles/white-house-hosts-summit-artificial-intelligence-american-industry/ Summary of report. And https://www.whitehouse.gov/wp.../Summary-report-of-White-House-AI-Summit.pdf

Whitney, L. (2016). 'Fitbit Still Tops in Wearables, but Market Share Slips' C/Net 12/02/16 Available from: https://www.cnet.com/uk/news/fitbit-still-tops-in-wearables-market/

Wilson, H. J. (2013). Wearables in the workplace. Harvard Business Review (Sep.). Available from: https://hbr.org/2013/09/wearables-in-the-workplace

Wilson, C. (2014). Interview Techniques for UX Practitioners: A User-Centred Design Method. Elsevier. Available from: https://doi.org/10.1016/C2012-0-06209-6

Woodcock, J. (2016). Working the phones: Control and Resistance in Call Centres. London: Pluto Press.

Yeung, K. (2017). Algorithmic Regulation: A Critical Interrogation. Regulation and Governance 2(4), 429-540.

Yin, R. K. (2014). Case Study Research: Design and Methods. Fifth Edition. Applied Social Science Research Methods Series Vol. 2. United States of America: Sage Publications.

Yin, R. K., Davis, D. (2007). Adding new dimensions to case study evaluations: The case of evaluating comprehensive reforms. New Directions for Evaluation, 113, 75 – 93.

Zajonc, R. B. (1965). Social facilitation. Science, 149, 269-274.

Zirkle, B. L., Staples, W. G. (2005). Negotiating Workplace Surveillance. In Weckert, J. (ed.) Electronic Monitoring in the Workplace: Controversies and Solutions, Melbourne: Idea Group Publishing, 79–100.

Zuboff, S. (1988). In the Age of the Smart Machine: The Future of Work and Power. New York: Basic Books.

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

OA-02-20-870-EN-N

This report provides an in-depth overview of the social, political and economic urgency in identifying what we call the 'new surveillance workplace'. The report assesses the range of technologies that are being introduced to monitor, track and, ultimately, watch workers, and looks at the immense changes they imbue in several arenas.

How are institutions responding to the widespread uptake of new tracking technologies in workplaces, from the office, to the contact centre, to the factory? What are the parameters to protect the privacy and other rights of workers, given the unprecedented and ever-pervasive functions of monitoring technologies?

The report evidences how and where new technologies are being implemented; looks at the impact that surveillance workspaces are having on the employment relationship and on workers themselves at the psychosocial level; and outlines the social, legal and institutional frameworks within which this is occurring, across the EU and beyond, ultimately arguing that more worker representation is necessary to protect the data rights of workers.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

ISBN 978-92-846-7280-6 | doi: 10.2861/879078 | QA-02-20-870-EN-N