social sciences

MDPI

Article

Insight or Intrusion? Correlating Routinely Collected Employee Data with Health Risk

Mark J. Taylor * and Megan Prictor

Melbourne Law School, University of Melbourne, Melbourne, VIC 3010, Australia; megan.prictor@unimelb.edu.au

* Correspondence: taylor.m@unimelb.edu.au

Received: 26 August 2019; Accepted: 15 October 2019; Published: 16 October 2019

Abstract: The volume, variety and velocity of data available to companies about their employees is already significant and likely to increase. Employers hold data about employees that could be used to explore the relationship between workplace practice in their organisation and risks to employee health. However, there is significant uncertainty about whether employers subject to English law are permitted to use this data for this purpose, and even whether they may be under a legal obligation to do so. In this article, the question of whether employers are legally permitted or legally obliged to use employee data to identify associations between workplace practice and risk to employee health is answered through an analysis of two spheres of English Law: data protection law, and health and safety law. The authors establish a hypothetical case study concerning a company that wishes to use employee data in this way, to illuminate a set of detailed legal issues. In particular, the question of whether a reasonable and prudent employer is under an obligation under health and safety law to use the data and analytic tools at his or her disposal to assess risk and inform his or her actions is considered. Also addressed is the question of whether such processing would satisfy the data protection law principles of "lawful, fair, and transparent" processing and that of "purpose limitation". A complex picture emerges. The analysis reveals that data protection legislation may not support a trend towards the re-use of employee data to enhance workplace health and safety; nor is there currently a clear mandate that responsible employers use data in this way. The line between useful insight into workplace practices and intrusion into employees' privacy remains blurred.

Keywords: data protection; employee data; health and safety at work

1. Introduction

The intense datafication of the working environment is overlaid by new possibilities brought about by rapid technological advance and developments in artificial intelligence and machine learning. This creates new ways of identifying patterns of workplace practice associated with risk of poor mental and physical health and workplace absence. As we realise this possibility in the workplace, we need to be able to articulate what good practice by employers looks like, given the respective rights and responsibilities of employees and employers. Within the many questions that are raised, this article isolates and examines a cluster of questions relating to what an employer may, or perhaps must, do with personal employee data originally collected for other purposes, but now available to help profile the health risks associated with their organisation's workplace practice. We aim to analyse this potential use of employee data by employers through the lens of current English law, in the two areas of occupational health and safety, and data protection. In doing so, we seek to answer the question: if employers are able to identify "unhealthy" practice in their organisations, using data they already collect, then are they permitted (by data protection law) or even required (by occupational health and safety law) to do so? The intersection between these two areas of law is important for any employer

seeking to use information relating to identifiable employees to assess how the workplace contributes to risk of poor health outcomes for employees. To focus our analysis of the law as it applies to the re-use of employee data by employers in this way, we present a hypothetical case study. Let us imagine a company that is interested in taking advantage of the opportunities that emerging technology provides. They want to better understand current practice in their organisation and the implications this has for employee health risk. Let us call them Forward-Looking Company ("FLC").

There are some workplace practices known to be associated with poor health outcomes for employees that are understood to be contingent on circumstance. These circumstances include those pertaining to an organisation's work patterns and "norms of responsiveness" (Barley et al. 2011, p. 903). They also include individuals' expectations and behavioural norms (Stich et al. 2019). FLC, armed with a recognition that the relationship between workplace practice and employee health risk will turn both on workplace culture and on individual expectations, want to apply insights to their own organisation. They want to use and link data they already collect about their employees:

(a) to learn more about current workplace practice,
(b) to check and improve their understanding of the connection between that practice and risk to employee health, and
(c) to inform the design of corrective action to reduce risk.

Our analysis will consider whether data protection legislation in England *allows* FLC to do this. It will also evaluate whether health and safety legislation *requires* them to do so. Finally, if they do use and link the existing data in this way to improve employee welfare, then can they also use any insight for the company's commercial benefit?

The aim of this article is to answer some of the critical questions facing FLC, or any company subject to English law, looking ahead to further and future uses of the data they hold, in order to inform an understanding of the relationship between workplace practice and risk to employee physical and mental health (which we describe as "the practice/risk relationship"). Much has been written about workplace surveillance (Ball 2010; Tredinnick and Laybats 2019; Edwards et al. 2018), and some consideration has previously been given to employee monitoring in the context of English Law (Jeffery 2002) and European Union (EU) data protection (Aloisi and Gramano 2019; Edwards et al. 2018). However, the following questions have not been addressed.

(1) Do companies, given their legal obligations to employees' health and safety, have a responsibility to use the data they hold: (a) to better understand the practice/risk relationship; and (b) to identify individual employees who may be at particular risk of harm?
(2) Under what conditions does United Kingdom (UK) data protection legislation permit an employer to use data, originally collected for other purposes, to better understand the practice/risk relationship?
(3) To what extent are the legal obligations and permissions described under (1) and (2) consistent?
(4) To what extent does the answer vary if the data is used for commercial benefit rather than employee welfare?

The importance of these questions stems from the likelihood that the data enabling such analysis will only become more available, to more companies, along with the tools necessary to analyse it quickly and with greater confidence in results. As increasingly rich and varied data is collected, and the technical opportunities to mine data for insight become more accessible and affordable, new functions will be offered to employers by the software industry. Increasingly, companies will need certainty about when, and for what purposes, they can deploy enhanced functionality across their systems to release the value that is hidden deep within data they already hold. It is important from a regulatory perspective to know whether the responsibilities employers are subject to under data protection law and health and safety law are mutually supportive or in conflict in ways that might undermine achievement of regulatory objectives. The article advances understanding of English data

protection law's (at times unhelpful) relationship with occupational health and safety legislation. It illuminates the difficulty facing an employer in seeking to go beyond currently established practice.

The article is organised as follows. We begin by further contextualising the problem of a changing work environment and the relationship between work and health. We then assess whether there may be an obligation under the UK Health and Safety at Work Act (1974) to use available data and analytics tools to better understand the relationship between workplace practice and employee risk. Establishing this to be a likely direction of travel, but not a current legal obligation, we then move to assess whether such processing is consistent with data protection responsibilities. Here the focus is on two principles: first, that processing must be "lawful, fair, and transparent" and second, that data collected for one purpose cannot be used for a new unrelated purpose unless certain requirements are met: the "purpose limitation" principle. Throughout, we consider uses an employer might make of any insight gained through the data analysis, compared with the impact of this activity—the intrusion—on the privacy that employees might reasonably expect (Article 29 Working Party 2017).

2. Changing Work Environment

The working environment is experiencing a rapid and seemingly relentless process of datafication. Increasingly, aspects of working lives are being turned into interpretable data, and the future workplace may be characterised by hyper-surveillance and pervasive rating systems (Dellot et al. 2019, p. 7). Research conducted by the Trades Union Congress (TUC) in 2018 identified that more than 50% of workers surveyed believed they were subject to monitoring at work, most commonly monitoring of email, phone calls and via closed-circuit television (CCTV). Workers also believed that more advanced forms of surveillance, such as location tracking devices and facial recognition software, were becoming more prevalent (Trades Union Congress (TUC)).

The motivations for capturing data on employees are likely to be diverse. Some capture will be incidental to the delivery of necessary business functions, e.g., to provide an email service to employees or to enable user authentication. In other cases, data may be deliberately captured to provide insight into employee performance. A current example is "Humanyze" employee badges, which capture data about location and interaction through a combination of accelerometer, bluetooth, infrared sensors and microphone (2018). Amazon is reported to have patented the design for wristbands that can pinpoint the location of warehouse employees and track their hand movements in real time (Ong 2018). New surveillance techniques are reported to include monitoring social media accounts and tracking exercise and sleep patterns (Tredinnick and Laybats 2019).

Whether data is collected by a company intentionally to monitor employee performance or incidentally to its other business functions, the concern of this article is whether this data may then be analysed to yield insight into the practice/risk relationship, when such analysis was *not* the original purpose of data collection. Most employers will have data of this kind. Even the most responsible amongst them may not have yet considered whether they can, or ought to, use the data they already hold to explore the practice/risk relationship. Yet there is ample reason to think that data routinely being collected about employees for other purposes could be repurposed to reveal risks to employees in general (as a group) or in particular (through individualised risk profiles).

3. Relationship between Work and Health

A glimpse into the possible future of hyper-surveillance and the potential it may offer for insight into health risk is provided by the software known as Isaak by the company StatusToday. Marketed as an "AI [artificial intelligence] that gives you people analytics to drive organisational change", Isaak is said to provide contemporaneous insights into employee wellbeing including email overload, work completed outside of office hours, and other signs of overwork (StatusToday 2019).

Companies routinely collect information about employee email use. Systems can be asked to report data about when employees are checking email outside of normal working hours, how frequently they check, how long it takes them to respond, and so on. There is also increasing use of sentiment

analysis of workplace emails. This information can be linked to what is already known about indicators of stress and burn out and it may be linked with other routinely collected data.

Routine data collection is being extended by a proliferation of sensors within the workplace, capturing physical movement, facial expression (affect recognition), and in some cases via biosensors providing data that could be analysed to reveal information about health, illness, mood and behaviour (Wongchoosuk et al. 2009; Mostrous and Brown 2008). Corporate wellness programmes record employee steps and provide access to "wellness apps" or websites offering health information. Systems can track and record employees' internet search queries, potentially yielding health insights regarding individuals and groups, such as yet-unannounced illness or pregnancy (Zarya 2016).

Overall, there is little doubt that an upward trend exists in the volume, variety and velocity of data available to an employer that could be used and linked to provide insight into physical and mental wellbeing. The value of such data will drive analytics companies to find ways to offer employers new services, such as Isaak, and repurpose data that systems already collect. Of course, employers may then use the resulting insights in different ways; for instance to increase productivity rather than enhance employee wellbeing (Booth 2019).

In Whose Interests?

Companies like FLC might have employees' interests at heart, but this need not be the case. Insight into the practice/risk relationship could be applied for purely commercial return with negative consequences for current or future employees. In our example, if FLC are aware that a significant minority of employees are seeking mental health help, then the company might seek to better understand the causative factors and the characteristics of those most vulnerable. This could help FLC to discharge a duty of care to those individuals and improve working conditions for all FLC employees. However, the company might also seek to identify the characteristics of those employees who seek help so that, in future, FLC can preferentially employ those without such characteristics. There are reports of health data being gathered surreptitiously to defend against claims of workplace injury. If a company can demonstrate an individual is predisposed to develop a condition, such as carpal tunnel syndrome, then they may seek to avoid liability for injury (Associated Press 2001). The imperfect alignment of employer and employee interests will fuel suspicion that insights gained through the introduction of new technology or data analytics will not (always) be used to the employees' advantage. This concern is long-standing. In the 1980s the Wall Street Journal "raised the prospect that computer surveillance may turn the automated office into a sweatshop" (cited by Attewell 1987, p. 87). The very perception of surveillance may itself be damaging if it increases levels of stress and anxiety or otherwise undermines employer–employee relations.

4. What Is Lawful?

To address the questions outlined above, we will examine English law in two key areas. In each area, we will consider how the law applies to the given case study, before drawing conclusions about whether the purported data processing is lawful, or even whether it may be legally required. There is much law that could be considered, but we will focus on the areas of data protection law and the law relating to health and safety at work. These are the legal regimes most likely to apply to data processing affecting most employees (as opposed to discrimination law, for example, that may have application in a more limited range of circumstances). This analysis is also needed because these two regimes may point in different directions, with health and safety law supporting use of employees' personal data to meet obligations to provide a safe workplace environment, while data protection law may restrict such use.

We first consider whether employers have a duty to use employee data to evaluate the practice/risk relationship in their own organisations. We then go on to consider whether employers can proceed with the type of processing we have outlined above, whilst meeting obligations under data protection law.

The Law Pertaining to Health and Safety at Work

In the UK, the Health and Safety at Work Act (1974) places a responsibility upon employers to manage and control risk in the workplace. It is a general duty of every employer to ensure, "so far as is reasonably practicable, the health, safety and welfare at work of all his employees" (S2(1) Health and Safety at Work Act 1974). This includes,

> The provision and maintenance of a working environment for his employees that is, so far as is reasonably practicable, safe, without risk to health, and adequate as regards facilities and arrangements for their welfare at work.
>
> (S2(e) Health and Safety at Work Act 1974)

Employers' duty is extended under secondary legislation entitled the Management of Health and Safety at Work Regulations 1999/1342, to include a suitable and sufficient assessment of the risk to employees' health and safety whilst they are at work (Regulation 3(1)(a)) and to arrangements for,

> The effective planning, organisation, control, monitoring and review of the preventive and protective measures.
>
> (Regulation 5)

The risk has been determined to include risk to mental as well as physical health (Walker v Northumberland County Council 1995).[1] Employers are thus responsible for assessing risk and for monitoring and reviewing the preventive and protective measures implemented to address it. That is, the monitoring responsibility is, specifically, the responsibility to monitor the measures put in place. The responsibility to identify the risk is implied by the duty to conduct a risk assessment and the more general duty to provide and maintain a safe and adequate working environment.

It is also a general duty of an employer to provide written notice of its general policy with respect to the health and safety of employees at work (S2(3) Health and Safety at Work Act 1974). The regulations further specify that employers must provide employees with "comprehensible and relevant information" on:

(a) The risk to their health and safety identified by the assessment;
(b) The preventive and protective measures. (Regulation 10)

If an employer were to implement a data-driven initiative to prevent and protect employees from poor health outcomes associated with specific workplace practices, then they would be under a responsibility to monitor and review the impact of such an initiative. They would also be under a responsibility to provide employees with "comprehensible and relevant information" about the preventive and protective measures being taken. This would complement the responsibilities regarding transparency of data processing under data protection legislation described later.

If employee representatives have been appointed, it is the duty of an employer to consult them with a view to effective co-operation in,

> Promoting and developing measures to ensure the health and safety at work of the employees, and in checking the effectiveness of such measures.
>
> (S2(6) Health and Safety at Work Act 1974)

This clearly moves beyond mere notification, toward co-production of measures regarding health and safety. The net effect is that employers undertaking a programme of work intended to explore the relationship between workplace practice and employee health and safety risk, or acting upon the

---

[1] In *Walker* an employer was held liable in relation to recurrence of a stress-induced mental condition.

insights derived from such a programme, should give employees information about the initiative and should monitor and review its effect. If employee representatives have been appointed, they should be engaged throughout. This should help to mitigate risks associated with scepticism regarding an employer's motives. This does not, however, answer the question of whether an employer is under a responsibility to use data they hold to assess the practice/risk relationship, e.g., as part of any requirement to carry out a suitable and sufficient risk assessment.

An employer's liability in relation to harms, including stress-related harms, will depend in part on the "reasonable foreseeability" of the harm to the employee by the employer. In Hatton v Sutherland (2002) the House of Lords confirmed the usual principles to be applied to claims relating to workplace injury, whether affecting physical or mental health, as set out in Stokes v Guest (1968):

> . . . the overall test is still the conduct of the reasonable and prudent employer, taking positive thought for the safety of his workers in the light of what he knows or ought to know; where there is a recognised and general practice which has been followed for a substantial period in similar circumstances without mishap, he is entitled to follow it . . . ; but, where this is developing knowledge, he must keep reasonably abreast of it and not be too slow to apply it. (para. 1783)

This would suggest that at present, and given workplaces' current "recognised and general practice", a company such as FLC would not be under a legal duty to take advantage of new methods of data analysis to search for fresh insight into the practice/risk relationship. This is the case only for as long as the relationship between practice and risk is not something they *ought to know* as a reasonable and prudent employer.

This case makes clear that an employer "must keep reasonably abreast" of developing knowledge. They must not be "too slow" to apply it. "Recognised and general practice" may change. If software widely deployed on information systems comes to have the capacity to flag relevant associations between practice and risk, and the use of such systems becomes commonplace, then there may be a shift in what it is reasonable to hold that an employer *ought to know*. If, in future, data is held by FLC that could alert it to the practice/risk relationship, the company has ready access to the means to distil that insight, *and* those means are regularly employed by others in the same industry, then FLC might be considered to be failing in their duty of care to employees if they do not extract that insight and act upon it.

Insight into the possible future direction of English law can be derived from comparable jurisdictions. We may consider relevant the recent Australian case of Westgem v Commonwealth Bank of Australia (2018). The case considered the admissibility of a data file into evidence and the question of whether a report prepared using data stored on the data file was a "book" kept by a body corporate for the purposes of relevant legislation. While in many ways far from the current question, what is interesting is the decision by the Court to admit the data file as evidence, and the software generated reports, even though they had been generated *after* litigation commenced. A report on the case noted that,

> . . . it follows that directors might be found to have failed in their duty of care and diligence when making a decision if information contained in files could have been distilled and used to make a better decision. (Gilbert and Tobin 2018)

We may be moving toward a position where an employer's failure to use routinely-collected data to identify the relationship between practice and risk is a failure to meet their statutory duty to suitably and sufficiently assess risk. If harm is "reasonably foreseeable" given what an employer *ought to have known* through the data and analysis readily available to them, then a failure to conduct themselves as a reasonable and prudent employer may leave them liable for resulting harm.

FLC, wishing to use progressive methods to identify risks to employees and target personalised interventions, might prefer to act in advance of legal requirements to do so, and to begin to use the

data they routinely collect in this way. The question we turn to now is whether FLC can conduct such an analysis without breaching data protection legislation. Under what conditions does data protection legislation permit an employer to use data, originally gathered for other purposes, to better understand the practice/risk relationship? To what extent does the legislation then control the application of any insight gained?

5. Data Protection Legislation

In the UK, relevant data protection legislation is established by an interplay between the Data Protection Act 2018 and The General Data Protection Regulation (GDPR) (EU 2016/679). It applies to *any* processing[2] of personal data, which itself is defined very broadly to include *any* information relating to an identified or identifiable person.[3] Data protection legislation places requirements upon data controllers to adhere to a set of data protection principles in the processing of personal data. Most employers will be "data controllers" for the data processed within their organisation: they determine the purpose and means of processing personal data relating to their employees. Principles of processing relate to "lawfulness, fairness, and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", "integrity and confidentiality", and "accountability" (Article 5 GDPR). We will consider two principles, "lawfulness, fairness, and transparency" and "purpose limitation", to illustrate some of the key hurdles that an employer would have to clear before they could lawfully use data originally collected for other purposes to analyse the practice/risk relationship.

We begin by considering the requirements for fair and lawful processing. Consideration of whether processing is fair and lawful requires us to give attention to the circumstances under which health data, as a special category data, may be processed. We then move on to consider the second limb of the first data protection principle: transparency, before finally considering the implications of the principle of "purpose limitation". For reasons of space we will not consider the full range of principles of data protection law that may be considered relevant, such as those relating to accountability. As will be seen, cumulatively the requirements to process "lawfully, fairly, and transparently" and consistent with the principle of "purpose limitation" might already present some challenges to an employer wanting to use personal data in the way proposed for FLC.

6. Fair and Lawful

The lawfulness of processing is determined, in part, by Article 6 of the GDPR. It is necessary, but not sufficient, to meet one of the conditions set out in Article 6(1). They include that the processing:

(i) has the data subject's consent (Article 6(1)(a)),
(ii) is necessary for the performance of a contract to which the data subject is party (Article 6(1)(b)),
(iii) is necessary for compliance with a legal obligation (Article 6(1)(c)), or
(iv) is necessary for the purposes of a data controller's legitimate interests (Article 6(1)(f)).

There are other conditions set out in Article 6(1) besides these, but these four are those most likely to be relevant to the question considered here. In addition to meeting one of the specific conditions set out in Article 6(1), the processing must also be otherwise fair and lawful. These will be considered in turn.

i. Consent (Article 6(1)(a))

---

[2] Broadly defined by Article 4(2) to include any operation or set of operations performed on personal data or on sets of personal data whether or not by automated means.

[3] Article 4(1) GDPR defines 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Because of the features of the employment relationship, "consent" is not usually the most appropriate legal basis for an employer to rely upon. This was clearly stated back in 2001 by the body responsible for providing authoritative guidance on EU data protection legislation, the Article 29 Working Party (Article 29 Working Party 2001, p. 3). The difficulty is that data protection law requires consent to be "free". It is only appropriate to rely upon consent where an employee has a genuinely free choice whether or not to give consent, and is able to withdraw that consent without detriment. Since the Article 29 Working Party issued this guidance (and complementary guidance in 2017), data protection legislation has been updated to, if anything, heighten the threshold for valid consent. The data protection regulator in the UK, the Information Commissioner's Office, has issued guidance that reiterates the view that consent will only be an appropriate basis for processing if people can be offered a genuine choice. The guidance recognises this may not be the case if the data controller is in a position of power over the other person, with the examples being a public authority or an employer processing employee data (Information Commissioner's Office n.d.; See also Recital 43 GDPR).

As the concern in this article is with the use of personal data originally routinely collected by an employer for other reasons, it is unlikely that consent will have been the most appropriate lawful basis for the original processing. It *may* be possible for an employer to demonstrate that, in relation to any *further* processing of personal data, for these specific purposes, there is a positively expressed, genuinely free, choice on the part of an employee.[4] Indeed, this might be the most effective way to prevent any uses of personal data which disadvantage an employee, as they would be free to reject them without adverse consequences. However, there are alternatives to employee consent that an employer may rely upon to establish a lawful basis for processing personal data under Article 6. Given that the power imbalance and dependency may make it difficult for an employer to establish the requisite degree of freedom with sufficient certainty, FLC may want to consider whether an alternative legal base may be relied upon for the purposes of satisfying the Article 6 requirement.

ii. Necessary for Performance of a Contract (Article 6(1)(b))

In specific cases, an employer may rely upon the fact that processing of employee data is necessary to the performance of the employment contract e.g., in relation to pay-roll. This may extend to data relating to health status, for example, "where an employee has particular requirements which need to be accommodated so that they can perform their duties" (Cameron 2018). The kind of *further* data processing that we have described, to identify connections between workplace practice and risks to health, is unlikely to be necessary to the performance of an employment contract. Although it is possible for policies expressed through employee handbooks, such as policies on use of employee data and/or monitoring, to be incorporated into employment contracts (Department of Transport v Sparks 2016), a contractual variation will normally require employee consent (Wandsworth London Borough Council 1998).[5] Of course, FLC may still adopt a policy on the use of employee data; as we have already seen they will need to publish such a policy for other reasons. However, unless incorporated into the employment contract in such a way that would establish the processing to be necessary for performance of the contract, such a policy would not provide a lawful basis for processing under Article 6(1)(b).

iii. Necessary for Compliance with a Legal Obligation (Article 6(1)(c))

---

[4] This would not be the case if an employer considered themselves to be under a duty to process the data to identify behaviour associated with poor health. As discussed later in the article, this is not likely to be the case currently but may be in future.

[5] Lord Woolf opined: "The general position is that contracts of employment can only be varied by agreement. However, in the employment field an employer or for that matter an employee can reserve the ability to change a particular aspect of the contract unilaterally by notifying the other party as part of the contract that this is the situation. However, clear language is required to reserve to one party an unusual power of that sort". Furthermore, in some circumstances, an employer may be able to insist upon a change if they have a legal right to it.

Where processing is necessary for compliance with a legal obligation to which the controller is subject, for instance if it *were* necessary to meet an obligation under health and safety law, then the processing would have a lawful basis under Article 6. As noted above, however, it is not at all clear that a relevant obligation would (yet) be understood to exist.

iv. Legitimate Interests (Article 6(1)(f))

The legal basis for processing employee data that is perhaps most likely to be available to FLC right now is that processing is necessary in the "legitimate interests" of the data controller. "Necessity" is not to be interpreted too narrowly:

> The concept of necessity is not interpreted in the sense of an "absolute" necessity, but in the sense of a requirement to apply the principle of proportionality, balancing the employer's interests in data processing against those of the employee concerned. (Aloisi and Gramano 2019)

In other words, a legitimate interest on the part of an employer may be interpreted broadly,[6] but is not sufficient to override the rights and freedoms of employees (Article 6(1)(f)). Relevant Article 29 Working Party guidance is that a

> ... proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary. (Article 29 Working Party 2017, p. 23)

If FLC could demonstrate that processing was not only in their legitimate (e.g., commercial) interests but also—or at least sufficiently—in the interests of employees (as e.g., it enabled intervention and risk reduction), then "legitimate interests" may provide a legal basis for processing. The requirement for *only* proportionate interference with employee rights and freedoms may have the effect of prohibiting processing for purely commercial purposes where inconsistent with sufficient respect for employee interests. There would be interplay between an understanding of what was considered a proportionate interference with employee general privacy rights in the workplace, a court's understanding of "fair" processing, and an employee's "reasonable expectations". The latter will be shaped, in part, by what employees are told about the processing.[7]

v. Otherwise Fair and Lawful

All processing is subject to an overriding requirement that it be "fair". While it has been subject to some regulator and academic consideration (Butterworth 2018) the meaning of the word remains relatively untested. As a requirement it, alongside the notion of "reasonable expectation", provides context to any determination of whether an interference with employees' general privacy rights is proportionate. A reasonable expectation of privacy has emerged under English law as a principal test to determine whether a duty is owed under the law of confidence (Taylor and Wilson 2019). As noted earlier, the duty to act lawfully under data protection law extends to compliance with other legal requirements. If processing breaches a duty of confidentiality, then processing is not fair and lawful in terms of data protection legislation (The General Data Protection Regulation (GDPR)).[8]

---

[6] In the case involving Article 8 of the European Convention of Human Rights the European Court of Human Rights considered a legitimate purpose of a company to extend to "ensuring the smooth running of the company" (Bărbulescu v Romania 2017, p.30).

[7] Though for reflections on the limits of notice in shaping reasonable expectations see ECtHR case (Antović & Mirković v Montenegro 2017).

[8] In concluding its investigation into the disclosure of patient personal data to DeepMind Technologies Limited by Royal Free Foundation Trust, the Information Commissioner's Office (ICO) found it reasonable to conclude, on the basis of advice

7. Law of Confidence

There is a narrow and untested line of legal argument to support the notion that an employer who reuses personal information that they already lawfully hold, for a purpose that has not been authorised by an employee, would be liable for a breach of confidence or the tort of misuse of personal information (Vidal-Hall & Ors v Google Inc. 2014) if there has been an unjustified interference with the employee's reasonable expectation of privacy.[9] It seems likely that some kind of inequity would need to be present, beyond simple reuse of data to analyse the relationship between practice and risk. It might be an available line of argument if use of that insight was considered inequitable; for example, if it was applied to boost productivity in ways that seemed manifestly unfair to employees. It would not be a viable argument in any circumstances where employers were found to be reusing data in order to comply with the law (Hunter v Mann 1974). In summary, we suggest there is little chance that simply using data to analyse the relationship between risk and practice would breach confidence and thus fail the responsibility to process fairly and lawfully under data protection law.

8. Lawful Processing of Health Data (Article 9 General Data Protection Regulation (GDPR))

Special categories of data qualify for additional protections under data protection law. Special categories are defined, in Article 9 GDPR, to include genetic data, biometric data which allow for or confirm an individual's unique identity (including photographs) (Recital 51 GDPR), and data concerning health. Even if special category data (such as health data) has not been collected by a data controller, but instead inferred through further processing of other ordinary (i.e., non-special category) data held, then the further processing must still meet the requirements of Article 9.[10] If special categories of data are not processed consistent with the requirements of Article 9, then it will not be lawful. Article 9 thus imposes additional requirements for lawful processing in relation to health data. Analysis of the risk/practice relationship by FLC is likely to reveal at least some employees to be at particular health risk. As it will not be possible to anticipate *which* employees will be revealed to be at risk, it will be prudent to process data relating to all employees as though it may reveal data concerning health.[11] Such processing is prohibited unless one of a number of exceptions applies. The exceptions most likely relevant here may be "explicit consent", "preventive or occupational medicine", "research" or "employment law rights or obligations". We briefly consider each in turn.

i. Explicit Consent (Article 9(2)(a))

As noted above, an employer can only rely upon "explicit consent" as a lawful exception to the general prohibition on processing special category data if they can effectively demonstrate that an employee has a genuinely free choice whether or not to give consent, and is able to withdraw that consent without detriment (Article 29 Working Party 2001, p. 3). If an employer *could* demonstrate that an explicit consent was genuinely free, and neither refusal to consent nor withdrawal would have negative consequences for an employee, then this could provide an exception to the general prohibition on the processing of special category data. However, alternative legal exceptions (considered below)

---

supplied by the National Data Guardian, that "the Royal Free did not have a valid basis for satisfying the common law duty of confidence and therefore the processing of that data breached that duty. In this light, the processing was not lawful under the Data Protection Act 1998". (Information Commissioner's Office 2017).

[9] A narrow interpretation of *R (On Behalf of Source Informatics)* v *Department of Health* [2001] QB 424 is challenged in (Taylor 2015).

[10] The Information Commissioner's Office gives a relevant example in relation to the publication of annual reports and accounts for charities: "Annual reports and accounts are likely to contain personal data relating to, trustees, staff, donors and beneficiaries. Some of this may be special category data or, data from which special category data can be inferred with some degree of certainty. For example, if a mental health charity names or identifies beneficiaries in their annual report, it may be possible to infer with reasonable certainty that these individuals suffer from a specific mental health condition. To process special category data [the Office of the Scottish Charity Regulator] will need to be able to rely on an Article 9 (GDPR) condition to process this data." (Information Commissioner's Office 2019).

[11] 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

may have an advantage, from a company such as FLC's perspective, in terms of lower administration costs and higher levels of participation. They would permit use of data unless an employee positively objected, rather than requiring explicit consent.

ii. Preventative or Occupational Medicine (Article 9(2)(h))

Alternatives to explicit consent include where processing is necessary for " ... purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee" (Article 9(2)(h) GDPR). Additional conditions attach to such processing, including that processing must be carried out by someone, such as an occupational health professional, subject to professional requirements of confidentiality. Neither preventive nor occupational medicine are defined within data protection law. Analysis of existing employee data to inform understanding of association between practice and risk to physical and mental health might fall within the scope of occupational medicine. Facts to support such an argument are likely to include known associations being flagged so that occupational health and safety professionals may appropriately target interventions and support employee health and wellbeing. If, however, processing to detect *new* generalisable insight is by a data analyst without a professional duty of confidentiality, or insight is used to support commercially motivated acts rather than occupational health practice, then it would fall outside this exception. It might be relatively difficult for FLC to describe the initial processing of data, to assess the significance of the practice/risk relationship for employees, as processing for the purposes of "occupational medicine". At the outset it is unknown what kind of insights or risks will be revealed, what kind of corrective action they might imply, or that the best people to carry out such analysis would be occupational health professionals.

iii. Research (Article 9(2)(j))

If analysis is intended to reveal *new* insights into general associations between practice and risk, and it is unknown initially what will be revealed, then FLC might consider seeking to rely upon the exception available for (health) research.[12] Article 9(2)(j) provides an exception to the general prohibition on processing special categories of data where processing is necessary for research purposes. Reliance upon this brings with it a requirement for additional safeguards, which should be provided for under national law (Recital 156 GDPR). For example, according to UK law such processing must not be "likely to cause substantial damage or distress" (S19(2) Data Protection Act 2018) and also, pertinently,

> must not be carried out for the purposes of measures or decisions with respect to a particular data subject. (Data Protection Act(Data Protection Act) Data Protection Act 2018)[13]

This means that FLC could *not* ordinarily rely upon research as the exception for processing if the analysis is used to make decisions affecting a particular employee.[14] It may be possible for them to carry out analysis in order to inform policy of broader application. Again, this has not been tested in the kind of scenario envisaged, but it might permit an organisation to analyse data for insight into the practice/risk relationship where the intention is to inform general action, rather than specific and targeted intervention.[15]

---

[12] Recital 159 notes that for the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including, for example, technological development and demonstration, fundamental research, applied research and privately funded research.

[13] This does not apply in case of medical research approved by an ethics committee (of a type listed under S.19(4) DPA 2018). We are largely discounting this possibility for the sake of this analysis as a company's use of employee data would not normally be considered by any of the committees listed under S.19(4). As a route to lawful processing it would require separate consideration.

[14] Ibid.

[15] Arguably, that kind of targeted intervention might more closely resemble activity to support occupational health and strengthen that former line of argument.

FLC might then consider both the categories of "occupational medicine" and "research" as unsuitable, as they are cast more narrowly than the purpose of processing they intend. As they anticipate such processing may, in the future, become an obligation under employment law, could they rely upon an alternative exception?

iv. Employment Law Obligations and Rights (Article 9(2)(b))

FLC might seek to argue that they have an obligation as an employer that justifies the processing, which points to use of the exception under Article 9(2)(b) GDPR. This exception applies where processing is:

> necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. (Article 9(2)(b) GDPR)

There is, however, an important condition attached to this particular alternative. Such processing must be

> authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject. (Article 9(2)(b) GDPR)

As noted above, it seems unlikely that UK law would be considered currently to place FLC under a duty to process the data to meet their statutory duty of care to employees. If so, Article 9(2)(b) may in the future *become* an available exception for processing due to requirements of UK law, just as it may *become* a lawful basis for processing under Article 6. FLC would, however, need to identify the lawful basis before processing the data, and could not justify processing now on the basis that the processing may become a legal obligation at a later point. Providing information about the legal basis of processing would be part of the requirements regarding transparency.

As noted above, the first principle relating to the processing of personal data is that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). Even if processing is lawful and fair, to satisfy the first data protection principle it must also be transparent. This responsibility extends beyond providing information about the legal basis of processing.

9. Transparency

Data protection legislation places responsibilities on a data controller to provide information to various stakeholders about the processing of personal data. These are additional to the transparency requirements associated with health and safety law described earlier. Whether data is obtained directly from the data subject or via a third party a data controller must provide information about the categories of personal data concerned and "the purposes for which the personal data are intended as well as the legal basis for processing" (Article 13(1)(c); Article 14(1)(c)). There are specific expectations regarding the timeliness of this information (Article 13(1); 13(3); 14(3)). It would not be lawful for an employer to use data, routinely collected about its employees, to investigate the practice/risk relationship without providing information about this purpose and the legal basis for the processing. The employer must provide this information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 21(1)). Employees have the right to object to processing.[16]

---

[16] Under Article 21(1) a data subject has the right to object "on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) of (f) of Article 6(1), including profiling based on those provisions." As a reminder, points (e) and (f) of Article 6(1) relate to "performance of a task carried out in the public interest" and "legitimate interests" of the data controller, respectively. Reliance upon Article 6(f) is already limited where such interests are "overridden by the interests or fundamental rights and freedoms of the data subject". The effect of Article

Automated Decision Making, Including Profiling

If data processing involves any automated decision-making for employees, including profiling, then particular transparency responsibilities apply. In this case, employers must provide information about the existence of such automated decision-making and "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (Article 13(2)(f); Article 14(2)(g)).

Furthermore, Article 22(1) of the GDPR establishes that a data subject has the right not to be subject to a decision based purely on automated processing, including profiling, which has a legal or similarly significant effect on him or her. This does not apply where processing is necessary for a contract between data subject and data controller (Article 22(2)(a)) or the data subject provides explicit consent (Article 22(2)(c)). Where data relates to an individual's health (or other special category data), then additional conditions apply (Article 22(4)). These include the requirement that suitable safeguards are in place[17] and, importantly, restrict the available exceptions under Article 9(2) to either explicit consent (Article 9(2)(a)) or "reasons of substantial public interest" (Article 9(2)(g)).

If automated decision-making were genuinely in the employees' interests, then they could be provided with the opportunity to give explicit consent to the processing. What is interesting is what happens if an employer genuinely considers that profiling employees, for instance according to health risks associated with workplace practice, is an action any reasonable or prudent employer would take to discharge a duty of care, but employees do not consent to the use (for example, due to scepticism that use of the data will always be aligned with their interests). This is one of the ways that tension may be introduced between the rights and responsibilities articulated by data protection legislation and an employer's obligations to protect their workforce. In such a case, the courts would not expect a reasonable or prudent employer to act contrary to their responsibilities as a data controller. The only alternatives that seem to be open to an employer, if the processing fell into the category of profiling, would be to argue either that such processing was for reasons of "substantial public interest" or that it had no legal or similarly significant effect on an employee. Any effect (positive *or* negative) may mean that an employer is prohibited from profiling employees, without explicit consent or a substantial public interest argument, even where they consider this to be the most appropriate way to discharge a duty of care under health and safety legislation.

10. Purpose Limitation

As well as requiring that all processing be "lawful, fair and transparent" it is also a requirement that personal data collected for a specified, explicit and legitimate purpose may not be "further processed in a manner incompatible with those purposes" (Article 5(1)(b)).

As the scenario we have outlined involves the further use of data for a purpose beyond that originally conceived, it is important to consider whether this processing would accord with the principle of purpose limitation. Incompatibility may be assessed substantively, and may permit even "non obvious" repurposing of data if not incompatible with the original purposes of collection and a reasonable person would not find them unexpected, inappropriate or otherwise objectionable (Article 29 Working Party 2013, pp. 21–27). Recital 50 of the GDPR states that, to determine compatibility with the originally stated purpose of processing, a data controller should consider, among other things,

---

21(1) is thus to place the onus on the data controller to either stop processing or to demonstrate an overriding interest in case of an employee objection. This is likely to limit the extent to which an employer may continue to process data relating to a specific employee in case of his or her objection.

[17] Recital 71 indicates such safeguards should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

> . . . any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

If in the context of an employment relationship, it *could* be demonstrated that employees had a reasonable expectation that data would be used in this way, employee rights and freedoms were appropriately safeguarded *and* the consequences for employees were not inappropriate, then it is possible that data might be legitimately repurposed. As any processing is prospective, this requirement would need to be met in relation to the processing of both data yet to be collected but now to be processed for new purposes as well as data already held. However, the Article 29 Working Party has indicated that if an intended use of data is to inform "measures or decisions" taken with regard to data subjects, then such processing would "almost always" require free, specific, informed and unambiguous "opt-in" consent (Article 29 Working Party 2013, p. 46). An employer may be well advised to regard any such further processing operation as new and to ensure data protection responsibilities are met from the beginning. In so doing, they would not need to claim that *further* processing is compatible with the original purposes.

11. Discussion

This analysis has highlighted the very complex legal considerations facing a company such as FLC in considering whether they are permitted or even obligated to use data they already hold about employees to assess the relationship between workplace practice and risks to employee health and wellbeing, through the lenses of occupational health and safety law and data protection law. It appears at present that there are wide-ranging legal protections for employees in the proposed uses of the data, limiting the "intrusion" they may suffer but also limiting the "insight" the company may glean into the practice/risk relationship from data they already hold.

After analysing the available options under UK data protection law, FLC would most likely seek to establish a lawful basis for processing on the grounds that processing was necessary in the company's legitimate interests. This would introduce a proportionality test and should ensure that the fundamental rights and freedoms of employees are not overridden. Further processing would be subject to a purpose limitation test and no further processing would likely be deemed compatible with the original purposes of processing if the effect would be to inform measures or decisions impacting upon employees. Such processing would need to be considered as a discrete processing operation and satisfy all data protection requirements in its own right (and not rely upon "compatibility" with the original purposes). This would include a responsibility to be transparent about these purposes of processing. Transparency would be supplemented by requirements to provide comprehensible and relevant information, under law relating to health and safety at work. This would extend to providing information about the use of data that was not personal. The latter legal regime would also place FLC under a duty to co-operate with any appointed employee representatives.

Furthermore, processing would need to be "fair" as well as "lawful." In relation to the former assessment, it is open to English courts to consider whether any use of employee data would amount to breach of confidence or a tort of misuse of personal information. Employees would also have a right under data protection law to object to any processing they considered to be inappropriate. In combination, this would already seem to establish a comprehensive set of checks and balances on the use of employee data by FLC to investigate the practice/risk relationship. Obligations owed in relation to the processing of a *special category* of data would, however, further extend it.

Until a legal obligation to use data in this way has been established, FLC could not rely upon the processing as necessary to meet a legal obligation to establish either a lawful basis for processing or to establish an exception to the processing of a special category of data. Any processing of data

intended to analyse the relationship between practice and risk would likely reveal data from which health risk could be inferred and related to identifiable individuals within the workforce. As it could not be anticipated from the outset who this information would relate to, it would be prudent to treat all processing as the processing of special category data.

A company seeking to lead the pack and take advantage of new technology and opportunity to identify practice associated with health risk in particular must fulfil the "special category" requirements in GDPR Article 9. They must either seek explicit employee consent for the processing or rely upon the alternative exceptions that the processing is necessary for research purposes or for reasons of occupational medicine. Neither may seem a particularly easy fit if an initiative is intended to first provide generalisable insight and then to enable targeted action. What is more, they are largely mutually exclusive (as reliance on the research exception ordinarily prohibits the use of data to inform decisions about individuals, whereas occupational medicine seems to require it). A data-driven initiative that covers terrain mapped by both would have to carefully align different activity with each of these exceptions at different points in time and be careful to avoid either gap or overlap. An initiative that involved profiling would have an even narrower path to tread.

What is unclear is whether these additional controls would provide material advantage to an employee above the protections associated with satisfaction of the principles of "lawful, fair and transparent" processing and that of "purpose limitation". These principles would *already* allow the courts to take into account relevant considerations such as the proportionality of any interference, the reasonable expectations of data subjects based on their relationship with the controller, the consequences of the processing for the data subjects, and the existence of appropriate safeguards. It may seem that there is already ample opportunity to curtail uses of data that inappropriately prioritise commercial interests at the cost of employees or otherwise interfere with reasonable expectations of privacy at work. If the challenge of navigating the available exceptions to the further prohibition on the processing of special category data, or those associated with profiling, discourages a company such as FLC from understanding the practice/risk relationship, then this may be seen itself to be inconsistent with employees' interests.

In essence, our analysis has shown that:

- Health and safety at work legislation does not appear to place a current legal obligation on employers to use the data in this way.
- Processing must be fair and lawful (noting breach of confidence and the tort of misuse of personal information).
- The obligation of transparency requires that employees are provided with comprehensible and relevant information in a timely fashion.
- Employment law obligations and rights may in the future be a lawful basis for processing in this context and an available exception for processing health data.
- The limbs of data protection law currently likely to be most suitable for the intended data use are: processing in the company's legitimate interests (which introduces a proportionality test), and, for special category data such as health data, selecting the exception (e.g., explicit consent, research, preventative or occupational medicine) that is the best fit for the proposed use.
- Reliance on the currently available exceptions in relation to special category data limits use of employee data to analyse the practice/risk relationship.
- The purpose limitation principle is likely to mean that proposed data analysis must be treated as a new processing operation.

12. Conclusions: Insight or Intrusion?

As more data is collected, and kept, and the opportunities to analyse it become more accessible, companies will consider whether it is possible, or even necessary, to use employee data in new ways. Of course, when doing so, data protection and health and safety legislation are not the only laws with

which an employer needs to comply. Yet even restricting an analysis to these two areas of law in England, a complex picture emerges.

There are many diverse reasons why an employer might seek to carry out the kind of analysis posited here. They might be motivated by a desire to understand workplace factors impacting upon levels of sick leave and work absences, or to shift policy in ways that will improve general staff welfare and/or to reduce overall costs. An employer might be seeking to identify specific individuals in the workplace who would benefit from targeted support, for instance through information or behaviour change interventions. They might intend that their recruitment, redeployment, or promotion practices be informed by additional information about the profiles of individuals most likely to be able to withstand the stressors of a role without suffering mental or physical harm.[18] Finally, an employer might be motivated by a desire to gather information that will prove useful to defend any claims of work-related injury or to otherwise privilege the commercial interests of the company above the welfare interests of its employees. It is unlikely to be only one of these reasons.

The range of possible motives aligns with varying degrees of fit against the different legal bases available for data processing under English law. It may be possible to find an adequate fit in many, but not all, circumstances. A company's legitimate commercial interests cannot override the interests of employees in fundamental rights and freedoms, but they may be balanced against them in a way that permits only proportionate interference. In this way, the requirement to ensure that processing is "lawful, fair, and transparent" provides opportunity to prohibit uses of data seen by the courts to be inequitable and unfair. Under English law this opportunity is bolstered by the law of confidence and the tort of misuse of personal information. Although it has not been applied to date to circumstances where an individual's identity is protected, this could change.

Health and safety at work legislation is not yet recognised to require that companies conduct the type of data processing we have considered here. While we might want a progressive employer to use the data they collect, not (only) to improve their commercial position, but to improve conditions for their workforce, existing data protection legislation creates a challenging environment for an employer seeking to use data to identify associations between practice and health risks. This is because any effort to process personal data to yield insight into these associations is likely bring the processing into the realm of special category data, with its particular protections.

Unless an employer processes special category data with an employee's explicit consent, the exceptions they may rely upon to process this data are limited, even more so if the processing constitutes employee profiling. On the one hand, this may be considered a very good thing from an employee's perspective. Either they provide a genuinely free consent, or data may only be used (without automated decision making or profiling) for reasons of occupational health or research. In both latter cases, employees' interests are protected to some extent by the involvement of an occupational health practitioner who owes them a duty of confidentiality, or the requirement that research processing does not inform decisions made about individuals (or is separately subject to ethics committee review). What is more, the general principle of purpose limitation prevents further processing for incompatible purposes.

However, the processing that an employer wishes to undertake, to identify associations between workplace practice and health risk in their organisation, may not easily sit within either occupational health or research categories. If the processing is profiling, neither is available to them. If in the future we reach the point that "hyper-surveillance" is realised and systems such as Isaak become commonplace, then it may be that a reasonable employer would be expected to know the risks that data can be analysed readily to reveal. Performing such analysis and, through it, identifying relevant risk, would then be part of discharging a duty of care to their employees. Until we reach that point and

---

[18] While the opportunity to use routinely collected corporate data may be limited if an individual is an external applicant, those seeking a new position or promotion within a company may have already left a rich record that could be mined.

a legal obligation is imposed, data protection legislation does nothing to encourage such uses of data. Indeed, difficulties in fitting practice to the relatively narrow exceptions may cool progress toward the responsible use of data to provide relevant insight, without adding any effective safeguards against unjustified intrusion.

Author Contributions: Conceptualization, M.J.T.; writing—original draft preparation, M.J.T.; writing—review and editing, M.P.

Funding: This research received no external funding.

Acknowledgments: We acknowledge the extremely useful comments made on draft versions of this piece by Damian Clifford, Edward Dove, and Roger Brownsword. We are also very grateful for the editorial advice and support received from Carolyn Axtell.

Conflicts of Interest: The authors declare no conflict of interest.

References

Aloisi, Antonio, and Elena Gramano. 2019. Artificial Intelligence is Watching You at Work. Digital Surveillance, Employee Monitoring and Regulatory Issues in the EU Context. *Comparative Labor Law & Policy Journal*. forthcoming. Available online: https://ssrn.com/abstract=3399548 (accessed on 15 October 2019).

Anonymous. 2018. There Will be Little Privacy in the Workplace of the Future. *The Economist*. March 28. Available online: https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future (accessed on 24 September 2019).

Antović & Mirković v Montenegro. 2017. ECHR 365. Available online: https://www.statewatch.org/news/2017/nov/echr-judgment-Mirkovic-v.-Montenegro-camera-surveillance.pdf (accessed on 15 October 2019).

Article 29 Working Party. 2001. *Opinion on the Processing of Personal Data in the Employment Context*. WP 48. Brussel: European Commission, Available online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (accessed on 15 October 2019).

Article 29 Working Party. 2013. *Opinion 03/2013 on Purpose Limitation*. WP 203. Brussel: European Commission, Available online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (accessed on 15 October 2019).

Article 29 Working Party. 2017. *Opinion 2/2017 on Data Processing at Work*. WP 249. Brussel: European Commission, Available online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (accessed on 15 October 2019).

Associated Press. 2001. Burlington Northern Settles Suit Over Genetic Testing. *The New York Times*, April 19.

Attewell, Paul. 1987. Big Brother and the Sweatshop: Computer Surveillance in the Automated Office. *Sociological Theory* 5: 87–100. [CrossRef]

Ball, Kirstie. 2010. Workplace Surveillance: An Overview. *Labor History* 51: 87–106. [CrossRef]

Bărbulescu v Romania. 2017. (Application No. 61496/08). Available online: https://hudoc.echr.coe.int (accessed on 5 September 2017).

Barley, Stephen R., Debra E. Meyerson, and Stine Grodal. 2011. Email as a Source and Symbol of Stress. *Organization Science* 22: 887–906. [CrossRef]

Booth, Robert. 2019. UK Businesses Using Artificial Intelligence to Monitor Staff Activity. *The Guardian*. April 7. Available online: https://www.theguardian.com/technology/2019/apr/07/uk-businesses-using-artifical-intelligence-to-monitor-staff-activity (accessed on 26 August 2019).

Butterworth, Michael. 2018. The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework. *Computer Law and Security Review* 34: 257–68. [CrossRef]

Cameron, Fiona. 2018. GDPR Engaged by Work of Occupational Health and Safety Practitioners. Pinsent Masons Out-Law Analysis. Available online: https://www.pinsentmasons.com/out-law/analysis/gdpr-occupational-health-safety-practitioners-work (accessed on 26 August 2019).

Data Protection Act. 2018. Available online: http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (accessed on 15 October 2019).

Dellot, Benedict, Rich Mason, and Fabian Wallace-Stephens. 2019. The Four Futures of Work: Coping with Uncertainty in an Age of Radical Technologies. RSA. Available online: https://www.thersa.org/globalassets/pdfs/reports/rsa_four-futures-of-work.pdf (accessed on 24 September 2019).

Department of Transport v Sparks. 2016. EWCA Civ 360. Available online: http://www.bailii.org/ew/cases/EWCA/Civ/2016/360.html (accessed on 15 October 2019).

Edwards, Lilian, Laura Martin, and Tristan Henderson. 2018. Employee Surveillance: The Road to Surveillance is Paved with Good Intentions. Paper presented at Amsterdam Privacy Conference, Amsterdam, The Netherlands, October 5.

Gilbert and Tobin. 2018. A Gathering Storm—Director's Duties and the Use and Misuse of Data. Available online: https://www.gtlaw.com.au/insights/gathering-storm-directors-duties-use-misuse-data (accessed on 24 September 2019).

Hatton v Sutherland. 2002. EWCA Civ 76. Available online: http://www.thehrexchange.co.uk/wp-content/uploads/2012/06/HATTON-V.-SUTHERLAND.pdf (accessed on 15 October 2019).

Health and Safety at Work Act. 1974. Available online: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127510.pdf (accessed on 15 October 2019).

Hunter v Mann. 1974. 1 QB 767. Available online: http://static.aston.ac.uk/applet/protected/prof_ethics/briefing_confidentiality.pdf (accessed on 15 October 2019).

Information Commissioner's Office. 2017. Letter from ICO to Royal Free Foundation Trust. July 3. Available online: https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf (accessed on 26 August 2019).

Information Commissioner's Office. 2019. Response to the Scottish Government's consultation on Scottish Charity Law. Available online: https:ico.org.uk (accessed on 16 October 2019).

Information Commissioner's Office. n.d. Guidance on 'When is Consent Appropriate?'. Available online: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/ (accessed on 26 August 2019).

Jeffery, Mark. 2002. Information Technology and Worker's Privacy: The English Law. *Comparative Labor Law & Policy Journal* 32: 301–50.

Mostrous, Alexi, and David Brown. 2008. Microsoft Seeks Patent for Office 'Spy' Software. *The Times*. January 16. Available online: https://www.thetimes.co.uk/article/microsoft-seeks-patent-for-office-spy-software-h0dd5zmtfnt (accessed on 24 September 2019).

Ong, Thuy. 2018. Amazon Patents Wristbands that Track Warehouse Employees' Hands in Real Time. *The Verge*. February 1. Available online: https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees (accessed on 26 August 2019).

StatusToday. 2019. Available online: https://www.statustoday.com (accessed on 26 August 2019).

Stich, Jean-Francois, Monideepa Tarafdar, Patrick Stacey, and Sir Cary Cooper. 2019. Appraisal of Email Use as A Source of Workplace Stress: A Person-Environment Fit Approach. *Journal of the Association for Information Systems* 20: 2. [CrossRef]

Stokes v Guest. 1968. 1 WLR 1776. Available online: https://swarb.co.uk/stokes-v-guest-keen-and-nettlefold-nuts-and-bolts-ltd-qbd-1968/ (accessed on 15 October 2019).

Taylor, Mark J. 2015. R v Department of Health, ex parte Source Informatics [1999]. In *Landmark Cases in Medical Law*. Edited by Jonathan Herring and Jesse Wall. Oxford: Hart Publishing.

Taylor, Mark J., and James Wilson. 2019. Reasonable Expectations of Privacy and Disclosure of Health Data. *Medical Law Review* 27: 432–60. [CrossRef] [PubMed]

The General Data Protection Regulation (GDPR) (EU 2016/679). 2016. Regulation (EU) 2016/679. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed on 15 October 2019).

Trades Union Congress (TUC). 2018. I'll Be Watching You: A Report on Workplace Monitoring. Available online: https://www.tuc.org.uk/sites/default/files/surveillancereport.pdf (accessed on 24 September 2019).

Tredinnick, Luke, and Claire Laybats. 2019. Workplace Surveillance. *Business Information Review* 36: 50–52. [CrossRef]

Vidal-Hall & Ors v Google Inc. 2014. EWHC 13 (QB). pp. 68–70. Available online: https://www.5rb.com/wp-content/uploads/2014/01/Vidal-Hall-v-Google.pdf (accessed on 15 October 2019).

Walker v Northumberland County Council. 1995. 1 ALL ER 737, [1995] ICR 702. Available online: https://www.lawteacher.net/cases/walker-v-northumberland-county-council.php (accessed on 15 October 2019).

Wandsworth London Borough Council. 1998. IRLR 193. Available online: https://swarb.co.uk/wandsworth-london-borough-council-v-dsilva-and-another-ca-9-dec-1997/ (accessed on 15 October 2019).

Westgem v Commonwealth Bank of Australia. 2018. WASC 150. Available online: https://ecourts.justice.wa.gov.au/eCourtsPortal/(X(1)S(sn5wcab1ttycxqznbhq0bvoy))/Decisions/DownloadDecision/a5d9c827-5ebf-46d5-af1b-337f1172be15?unredactedVersion=False&AspxAutoDetectCookieSupport=1 (accessed on 15 October 2019).

Wongchoosuk, Chatchawal, Mario Lutz, and Teerakiat Kerdcharoen. 2009. Detection and Classification of Human Body Odor using an Electronic Nose. *Sensors* 9: 7234–49. [CrossRef] [PubMed]

Zarya, Valentina. 2016. Employers Are Quietly Using Big Data to Track Employee Pregnancies. Fortune. Available online: https://fortune.com/2016/02/17/castlight-pregnancy-data/ (accessed on 26 August 2019).